DoD 8320.1-M-1

DATA STANDARDIZATION PROCEDURES

APRIL 1998

THE OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE FOR
COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

April 2, 1998

FOREWORD

This Manual is issued under the authority of DoD Directive 8320.1, "DoD Data Administration," September 26, 1991. It prescribes procedures for the development, approval, and maintenance of DoD data standards necessary to support the policies of DoD Data Administration as established by DoD Directive 8320.1. DoD 8320.1-M-1, "Data Element Standardization Procedures," January 1993, is hereby cancelled.

This Manual applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components"). Its provisions are applicable to all new initiatives to develop, modernize, or migrate information systems, whether automated or nonautomated.

This Manual is effective immediately; it is mandatory for use by all the DoD Components.

Send recommended changes to the Manual to:

Center for Standards
Chief, Data Standards Division
10701 Parkridge Blvd.
Reston, VA 22091-4357

The DoD Components may obtain copies of this Manual through their own publications channels. The document also is available electronically under the heading "publications" at the following internet site: http://web7.whs.osd.mil/corres.htm. Approved for public release; distribution unlimited. Authorized registered users may obtain copies of this Publication from:

Defense Technical Information Center (DTIC)
8725 John J. Kingman Rd.
Suite 0944
Fort Belvoir, VA 22060-6218
Commercial telephone: 1-800-225-DTIC (1-800-225-3842)
msorders@dgif.dtic.mil

Other Federal Agencies and the public may obtain copies from:

U.S. Department of Commerce
National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161
Commercial telephone: 1-703-605-6000

Arthur L. Money
Senior Civilian Official

TABLE OF CONTENTS

FIGURES

REFERENCES

(a) DoD 8320.1-M, "Data Administration Procedures," March 1994 authorized by DoD Directive 8320.1, September 26, 1991
(b) Federal Information Processing Standards (FIPS) PUB 184, “Specifications for Integration Definition for Information Modeling (IDEF1X),” December 21, 1993
(c) DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992
(d) Federal Information Processing Standards (FIPS) PUB 11-3, "American National Dictionary for Information Systems," (adopted in entirety from American National Standards Institute (ANSI) X3.172-1990), February 1991
(e) Federal Information Processing Standards (FIPS) PUB 183, “Integration Definition for Function Modeling (IDEF0),” December 21, 1993
(f) DoD 8910.1-M, “DoD Procedures for Management of Information Requirements,” November 1986, authorized by DoD Directive 8910.1, August 1986
(g) DoD Directive 8320.1, "DoD Data Administration," September 26, 1991
(h) DoD 5000.2-R, "Mandatory Procedures for Major Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs," March 15, 1996 authorized by DoD Directive 5000.1, March 15, 1996
(i) Integration and Runtime Specification, Version 3.0, July 1, 1997
(j) Federal Information Processing Standards (FIPS) PUB 10-4, "Countries, Dependencies, Areas of Special Sovereignty, and their Principal Administrative Divisions," April 1995
(k) Federal Information Processing Standards (FIPS) PUB 5-2, "Codes for the Identification of the States, the District of Columbia and the Outlying Areas of the United States, and Associated Areas," May 28, 1987
(l) Federal Information Processing Standards (FIPS) PUB 55-3, "Codes for Named Populated Places, Primary County Divisions, and Other Locational Entities of the United States, Puerto Rico, and the Outlying Areas," December 28, 1994
(m) Federal Information Processing Standards (FIPS) PUB 9-1, "Congressional Districts of the United States," November 30, 1990
(n) Federal Information Processing Standards (FIPS) PUB 8-6, "Metropolitan Areas (including MAs, CMSAs, PMSAs, and NECMAs)," March 1995

DL1. DEFINITIONS

DL1.1.1. Activity Model. A model of the processes that make up the functional activity showing inputs, outputs, controls, and mechanisms through which the processes of the functional activity are (or will be) conducted. (See DoD 8320.1-M (reference (a)).)

DL1.1.2. Alternate Key. Any candidate key of an entity other than the primary key. (See FIPS PUB 184 (reference (b)).)

DL1.1.3. Approved Standard Data Element. A standard data element that has been coordinated through the standardization process and approved for use in DoD systems and models.

DL1.1.4. Associative Entity. An entity that inherits its primary key from two or more other entities and documents multiple associations (relationships) between those entities. An associative entity is also known as an intersecting entity.

DL1.1.5. Attribute. A property or characteristic that is common to some or all of the instances of an entity. An attribute represents the use of a domain in the context of an entity. (See FIPS PUB 184 (reference (b)).)

DL1.1.5.1. Key Attribute. An attribute that may be used to uniquely identify an instance of an entity or entity class.

DL1.1.5.2. Non-key Attribute. An attribute that is not the primary or a part of a composite primary key of an entity. A non-key attribute may be a foreign key or alternate key attribute. (See FIPS PUB 184 (reference (b)).)

DL1.1.6. Attributive Entity. An object that accommodates a repeating value for the parent object by appending an additional descriptive quality to the key structure of the accommodating object that does not appear in the descriptive qualities for the parent object. An attributive entity is a dependent entity with exactly one identifying parent. Attributive entities are created to support the first rule of normalization: eliminating repeating values from the parent entity. Also known as a characteristic entity.

DL1.1.7. Business Rule. A statement of fact that identifies constraints governing the business functions and information requirements of an enterprise.

DL1.1.8. Candidate Key. An attribute, or combination of attributes, of an entity whose values uniquely identify each entity instance. (See FIPS PUB 184 (reference (b)).)

DL1.1.9. Cardinality. A statement of the number of entity instances that may or must participate at each end of a relationship. (See Relationship). Cardinality is the combination of degree and nature.

DL1.1.9.1. Degree. An expression describing the number of instances of one entity that may be related to each occurrence of another entity at each end of the association from one entity to another.

DL1.1.9.2. Nature. An expression of the mandatory or optional quality of each end of the association from one entity occurrence to another entity occurrence.

DL1.1.10. Category Cluster. A set of one or more mutually exclusive categorization relationships for the same generic entity. (See FIPS PUB 184 (reference (b)).)

DL1.1.11. Category Discriminator. An attribute in the generic entity (or a generic ancestor entity) of a category cluster. The values of the discriminator indicate which category entity in the category cluster contains a specific instance of the generic entity. All instances of the generic entity with the same discriminator value are instances of the same category entity. The inverse is also true. (See FIPS PUB 184 (reference (b)).)

DL1.1.12. Category Entity. An entity whose instances represent a sub-type or sub-classification of another entity (generic entity). Also known as sub-type or sub-class. (See FIPS PUB 184 (reference (b)).)

DL1.1.13. Characteristic Entity. (See Attributive Entity)

DL1.1.14. Child Entity. The entity in a specific connection relationship whose instances can be related to zero or one instance of the other entity (parent entity). (See FIPS PUB 184 (reference (b)).)

DL1.1.15. Class Word. A word in the name of a data element (attribute) describing the category to which the data element belongs; e.g., "quantity," name," "code." The word establishes the general structure and domain of a standard data element.

DL1.1.16. Class Word Modifier. A word that is used to further refine or describe a class word. The class word modifier is optional and may be used with a class word to form a generic element. (See Generic Element)

DL1.1.17. Component Data Administrator. Responsible for managing and implementing data administration within their Component area. They are appointed by Component Heads.

DL1.1.18. Composite Data Element. A data element that is formulated to describe multiple concepts. A composite data element definition and meaning can easily partially overlap with the definition of another data element. This redundancy sets the stage for data inconsistencies, increases system maintenance costs, and restricts the use of a data element to a narrow range of applications.

DL1.1.19. Conceptual Schema. (See Schema - Conceptual Schema)

DL1.1.20. Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means.

DL1.1.21. Data Administration. That function of the organization that oversees the management of data across the enterprise and is responsible for central information planning and control.

DL1.1.22. Data Administrator (DAd). A person or group that ensures the utility of data used within an organization. Responsibilities include defining data policies and standards, planning for the efficient use of data, coordinating data structures among organizational components, performing logical database designs, and defining data security procedures.

DL1.1.23. Data Architecture. A framework for organizing the interrelationships of data, (based on an organization's missions, functions, goals, objectives, and strategies), providing the basis for the incremental, ordered design and development of systems based on successively more detailed levels of data modeling. (See DoD 8320.1-M (reference (a)).)

DL1.1.24. Data Definition Language (DDL). The language used to define physical data structures in a database management system.

DL1.1.25. Data Dependence. The property of data where the existence of the data depends on the existence of other pieces of data.

DL1.1.26. Data Dictionary. A specialized type of database containing meta-data that are managed by a data dictionary system; a repository of information describing the characteristics of data used to design, monitor, document, protect, and control data in information systems and databases; an application of a data dictionary system.

DL1.1.27. Data Element. (See Attribute)

DL1.1.28. Data Element Standardization. The process of documenting, reviewing, and approving unique names, definitions, characteristics, and representations of data elements according to established procedures and conventions.

DL1.1.29. Data Integrity. A property of data in which all assertions (accurate, current, consistent, complete) hold.

DL1.1.30. Data Model. A graphical and textual representation of analysis that identifies the data needed by an organization to achieve its mission, functions, goals, objectives, and strategies and to manage and rate the organization. A data model identifies the entities, domains (attributes), and relationships (or associations) with other data, and provides the conceptual view of the data and the relationships among data. (See FIPS PUB 184 (reference (b)).)

DL1.1.31. Data Object. A term used to refer to either an entity or an attribute.

DL1.1.32. Data Quality. The correctness, timeliness, accuracy, completeness, relevance, and accessibility that make data appropriate for use.

DL1.1.33. Data Requirements. A specification of entities, attributes, relationships and domain values needed to support a business function.

DL1.1.34. Data Standard. A specific data format that conforms to the requirements of this Manual; specifically an entity, attribute (data element), and entity relationship (business rule). The basic components of a data standard are a logical data model and meta-data.

DL1.1.35. Data Steward. The person or group that manages the development, approval, creation, and use of data associated with a specific data standard managed within a specified functional area.

DL1.1.36. Data Structure. A logical relationship that exists among units of data and the descriptive features defined for those relationships and data units; an instance or occurrence of a data model.

DL1.1.37. Database. A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; the data are stored so that they can be used by different programs without concern for the data

structure or organization. A common approach is used to add new data and to modify and retrieve existing data.

DL1.1.38. Database Administrator (DBA). A person or group that enforces policy on "how," "where," and "in what manner" data are stored and maintained in each database. Provides information to the data administrator on organizational use of data within the subject database. (See DoDD 8000.1 (reference (c)).)

DL1.1.39. Database Management System. A computer-based system used to establish, make available, and maintain the integrity of a database, that may be invoked by nonprogrammers or by application programs to define, create, revise, retire, interrogate, and process transactions; and to update, back up, recover, validate, secure, and monitor the database. (See FIPS PUB 11-3 (reference (d)).)

DL1.1.40. Degree. (See Cardinality)

DL1.1.41. Dependent Entity. An entity that depends on the existence of one or more other entities for its identification. The entities on which it depends can be either independent or dependent. The primary key for a dependent entity contains foreign keys contributed by the entities on which it depends. There are three basic types of dependent entities: category entity, attributive entity, and associative entity.

DL1.1.42. Derived Data Elements. Derived data elements represent the results of computational operations performed on other data elements. The computations may involve algorithms supported by two or more data elements within a single entity instance, or algorithms summarizing data element values across multiple entity instances within a single entity or across multiple entities.

DL1.1.43. DoD Data Administrator. Responsible for the overall management and execution of the Data Administration Program and for ensuring the technical correctness and consistency of data administration products as well as developing data administration procedures, handbooks, and training materials. (See DoD 8320.1-M (reference (a)).)

DL1.1.44. DoD Data Model. An integrated view of data requirements for the functional areas and Components in the Department of Defense.

DL1.1.45. DoD Joint Technical Architecture. The DoD Joint Technical Architecture (JTA) provides the "building codes" which, when implemented, permit the rapid and seamless flow of information among DoD's information systems in support of the Warfighter. The JTA identifies a common set of mandatory rules,

information technology standards, and guidelines to be used in all new and upgraded C4I acquisitions across DoD. The JTA standards are to be used for sending and receiving information (information transfer standards such as Internet Protocol suite), for understanding the information (information content and format standards such as data elements, or image interpretation standards) and for processing that information. The JTA also includes a common human-computer interface and rules for protecting the information (i.e., information systems security standards).

DL1.1.46. Domain. The set of permissible data values from which actual values are taken for a particular attribute or specific data element. In a relational database, all of the permissible tuples for a given relation.

DL1.1.47. Enterprise. The highest level in an organization; includes all missions and functions.

DL1.1.48. Entity. The representation of a set of real or abstract things (people, objects, places, events, ideas, combination of things, etc.) that are recognized as the same type because they share the same characteristics and can participate in the same relationships. (See FIPS PUB 184 (reference (b)).) (Also known as prime word.)

DL1.1.49. Entity Class. (See Entity)

DL1.1.50. Entity Type. (See Entity)

DL1.1.51. Entity Relationship Diagram (ERD). A graphic representation that presents major entities and their relationships.

DL1.1.52. External Schema. (See Schema - External Schema)

DL1.1.53. Facilitator. A person who’s declared role is to guide a meeting toward its objective (e.g., development of activity and data models for an organization).

DL1.1.54. Foreign Key. An attribute, or combination of attributes of a child or category entity instance whose values match those in the primary key of a related parent or generic entity instance. A foreign key results from the migration of the parent or generic entities primary key through a specific connection or categorization relationship. (See FIPS PUB 184 (reference (b)).)

DL1.1.55. Fully Attributed Model. A third normal form information model that includes all entities, attributes,

relationships, and integrity rules needed by the functional activity being modeled.

DL1.1.56. Functional Activity. The primary subdivision of a functional area, made up of a collection of processes that can be managed together using policies and procedures not specifically applicable to other functional activities within the functional area. (See DoD 8320.1-M (reference (a)).)

DL1.1.57. Functional Area. A functional area (e.g., personnel) is comprised of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews).

DL1.1.58. Functional Area Data Model. Business area model of data requirements that support specific information needs within or between the major functional areas of an enterprise. It is used for business area analysis to support functional area integration.

DL1.1.59. Functional Data Administrator. Responsible for the overall management and implementation of data administration within their DoD Functional Area . They are appointed by Principal Staff Assistants. They perform the role of data steward for the data within their functional area. (See DoD 8320.1-M (reference (a)).)

DL1.1.60. Fundamental Entity. (See Independent Entity)

DL1.1.61. General Domain. A specified range of values a data element is permitted to have. In general, these domains are too large to be completely enumerated easily. For example: The general domain of a data element named "PERSON BIRTH DATE" is any date falling in the range 1 Jan 1850 through the current date. Although the domain is constrained (e.g., possibly to refer to only people who are currently alive), there is a large number of values.

DL1.1.62. Generalization Entity. (See Generic Parent)

DL1.1.63. Generic Element. A generic element specifies a broad domain of data values. It represents a homogeneous set of data values that may be used with many objects. The attributes of a generic element characterize broad aspects of a variety of data elements. Generic elements may have general or specific domains of data. A generic element is comprised of a class word and optional class word modifier. (See Class Word and Class Word Modifier)

DL1.1.64. Generic Parent. The entity at the top of any level of a hierarchy of entities. The parent entity of a categorization relationship.

DL1.1.65. Group Attribute. An attribute that is a collection of other attributes called constituents.

DL1.1.66. IDEF. (See Integrated Computer Aided Manufacturing Definition)

DL1.1.67. IDEF0. A modeling technique used to produce a "function model". A function model is a structured representation of the functions, activities or processes within the modeled system or subject area. (See FIPS PUB 183 (reference (e)).)

DL1.1.68. IDEF1X. A modeling technique used to produce an "information model" that represents the structure and semantics of information within the environment or system. (See FIPS PUB 184 (reference (b)).)

DL1.1.69. Identifying Relationship. A specific connection relationship in which every attribute in the primary key of the parent entity is contained in the primary key of the child entity. (See FIPS PUB 184 (reference (b)).)

DL1.1.70. Independent Entity. An object of interest to the enterprise that can be identified using primary key attributes that characterize the object without referring to Foreign Keys migrated from any other entity. Also known as a fundamental, principal, primary, independent entity class, and supertype.

DL1.1.71. Independent Entity Class. (See Independent Entity)

DL1.1.72. Information. Any communication or reception of knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, including computerized databases, paper, microform, or magnetic tape.

DL1.1.73. Information Engineering. A disciplined methodology that creates an organization-wide architectural framework for application and database development.

DL1.1.74. Information Requirement. The functional area expression of need for data, information, or reports to carry out specified and authorized functions or management purposes, and which call for the establishment or maintenance (update) of data, information, reporting, or record keeping systems whether manual or automated. (See DoD 8910.1-M (reference (f)).)

DL1.1.75. Information Model. A model that represents the structure and semantics of information within the environment or system. (See FIPS PUB 184 (reference (b)).)

DL1.1.76. Information System. The organized collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

DL1.1.77. Integrated Computer-Aided Manufacturing Definition (IDEF). A technique used for modeling an enterprise's processes and data.

DL1.1.78. Integrity Constraint. A statement in an information model that specifies one or more assertions regarding how specific instances of data objects are captured and managed.

DL1.1.79. Internal Schema. (See Schema - Internal Schema)

DL1.1.80. Intersecting Entity. (See Dependent Entity and Associative Entity)

DL1.1.81. Key Attribute. (See Attribute)

DL1.1.82. Logical Data Model. A model of data that represents the inherent structure of that data and is independent of individual applications of the data and also of the software or hardware mechanisms which are employed in representing and using the data. (See DoD 8320.1-M (reference(a)).)

DL1.1.83. Meta-data. Information describing the characteristics of data; data or information about data; descriptive information about an organization's data, data activities, systems, and holdings.

DL1.1.84. Methodology. The principles, practices, etc., of orderly thought or procedure applied to a particular branch of learning (i.e., data modeling). A set of standards and procedures used to guide the development of a data model.

DL1.1.85. Modeling. Application of a standard, rigorous, structured methodology to create and validate a physical, mathematical, or otherwise logical representation of a system, entity, phenomenon, or process. (See DoD 8320.1-M (reference(a)).)

DL1.1.86. Nature. (See Cardinality)

DL1.1.87. Non-identifying Relationship. A specific connection relationship in which some or all of the attributes contained in

the primary key of the parent entity do not participate in the primary key of the child entity. (See FIPS PUB 184 (reference (b)).)

DL1.1.88. Non-key Attribute. (See Attribute)

DL1.1.89. Non-standard Data Element. A non-standard data element is ny documented data element which does not comply with the standardization criteria of the 8320 series.

DL1.1.90. Non-specific Relationship. A relationship in which an instance of either entity can be related to a number of instances of the other. (See FIPS PUB 184 (reference (b)).)

DL1.1.91. Normal Form. The condition of an entity relative to satisfaction of a set of normalization theory constraints on its attribution. A specific normal form is achieved by successive reduction of an entity from its existing condition to some more desirable form. The procedure is reversible.

DL1.1.91.1. First Normal Form (1NF). An entity is in 1NF if and only if all underlying simple domains contain atomic values only. Each attribute of an entity must have exactly one value for each instance, with no lists, repeated occurrences, nor internal structures.

DL1.1.91.2. Second Normal Form (2NF). An entity is in 2NF if and only if it is in 1NF and every non-key attribute is fully dependent on the primary key.

DL1.1.91.3. Third Normal Form (3NF). An entity is in 3NF if and only if it is in 2NF and every attribute that is not a part of the primary key is a non-transitively dependent (mutually independent) on the primary key. Two or more attributes are mutually independent if none of them is functionally dependent on any combination of the others. (See FIPS PUB 184 (reference (b)).)

DL1.1.92. Normalization. The process of refining and regrouping attributes in entities according to the normal forms. (See FIPS PUB 184 (reference (b)).)

DL1.1.93. Null. A condition where a value of an attribute is not applicable or not known for an entity instance. (See FIPS PUB 184 (reference (b)).)

DL1.1.94. Parent Entity. An entity in a specific connection relationship whose instances can be related to a number of instances of another entity (child entity). (See FIPS PUB 184 (reference (b)).)

DL1.1.95. Physical Data Model. A representation of the technologically independent requirements in a physical environment of hardware, software, and network configurations representing them in the constraints of an existing physical environment.

DL1.1.96. Primary Entity. (See Independent Entity)

DL1.1.97. Primary Key. The candidate key selected as the unique identifier of an entity. (See FIPS PUB 184 (reference (b)).)

DL1.1.98. Prime Word. (See Entity)

DL1.1.99. Principal Entity. (See Independent Entity)

DL1.1.100. Property Modifier. A word that is used to further refine or describe an entity name or a generic element name.

DL1.1.101. Qualitative Data. A data value that is a non-numeric description of a person, place, thing, event, activity, or concept.

DL1.1.102. Quantitative Data. Numerical expressions upon which mathematical operations can be performed.

DL1.1.103. Relationship. An association between two entities or between instances of the same entity. (See FIPS PUB 184 (reference (b)).)

DL1.1.104. Relationship Name. A verb or verb phrase which reflects the meaning of the relationship expressed between the two entities shown on the diagram on which the name appears. (See FIPS PUB 184 (reference (b)).)

DL1.1.105. Role Name. A name assigned to a foreign key attribute to represent the use of the foreign key in the entity. (See FIPS PUB 184 (reference (b)).)

DL1.1.106. Schema. A definition of data structure:

DL1.1.106.1. Conceptual Schema. A schema of the American National Standards Institute's (ANSI) Standards Planning and Requirements Committee's (SPARC) Three Schema Architecture, in which the structure of data is represented in a form independent of any physical storage or external presentation format.

DL1.1.106.2. External Schema. A schema of the ANSI SPARC Three Schema Architecture, in which views of information are represented in a form convenient for the users of information; a description of the structure of data as seen by the user of a system.

DL1.1.106.3. Internal Schema. A schema of the ANSI SPARC Three Schema Architecture, in which views of information are represented in a form specific to the database management system used to store the information; a description of the physical structure of data. (See FIPS PUB 184 (reference (b)).)

DL1.1.107. Secondary Entity. (See Category Entity)

DL1.1.108. Specific Domain. The precise set of possible values for a data element (attributes).

DL1.1.109. Specific Connection Relationship. A relationship where a number of instances of one entity (child entity) can be related to zero or one instance of the other entity (parent entity). In a specific connection relationship, the primary key of the parent entity is contributed as a foreign key to the child entity. (See FIPS PUB 184 (reference (b)).)

DL1.1.110. Standard Data Element. A data element that has been coordinated through the standardization process and approved for use in DoD information systems.

DL1.1.111. Subentity. (See Category Entity)

DL1.1.112. Subtype Entity. (See Category Entity)

DL1.1.113. Supertype Entity. (See Independent Entity)

DL1.1.114. Technique. The working methods or manner in which rules, syntax, semantics are applied within a given methodology.

DL1.1.115. Tuple. A row in a table.

DL1.1.116. View. A collection of entities and assigned attributes (domains) assembled for some purpose. (See FIPS PUB 184 (reference (b)).)

AL1. ABBREVIATIONS AND ACRONYMS

AL1.1.1.	AIS	Automated Information System
AL1.1.2.	ANSI	American National Standards Institute
AL1.1.3.	ASCII	American Standard Code for Information Interchange
AL1.1.4.	ASD	Assistant Secretary of Defense
AL1.1.5.	C3I	Command, Control, Communications, and Intelligence
AL1.1.6.	CDA	Central Design Activity
AL1.1.7.	CDAd	Component Data Administrator
AL1.1.8.	CINC	Commander in Chief
AL1.1.9.	COTS	Commercial Off-The-Shelf
AL1.1.10.	DAd	Data Administrator
AL1.1.11.	DAdm	Data Administration
AL1.1.12.	DASD	Deputy Assistant Secretary of Defense
AL1.1.13.	DASP	Data Administration Strategic Plan
AL1.1.14.	DBMS	Database Management System
AL1.1.15.	DDDS	Defense Data Dictionary System
AL1.1.16.	DDL	Data Definition Language
AL1.1.17.	DDM	Department of Defense Data Model
AL1.1.18.	DIST	Defense Integration Support Tool
AL1.1.19.	DoD	Department of Defense
AL1.1.20.	DTIC	Defense Technical Information Center
AL1.1.21.	ERD	Entity Relationship Diagram
AL1.1.22.	FDAd	Functional Data Administrator
AL1.1.23.	FIPS	Federal Information Processing Standards
AL1.1.24.	IDEF1X	Integrated Computer-Aided Manufacturing Definition One Extended - Data Modeling Technique
AL1.1.25.	IM	Information Management
AL1.1.26.	IRM	Information Resource Management
AL1.1.27.	IS	Information System
AL1.1.28.	ISO	International Organization for Standardization
AL1.1.29.	JTA	Joint Technical Architecture
AL1.1.30.	NATO	North Atlantic Treaty Organization
AL1.1.31.	NIST	National Institute of Standards and Technology
AL1.1.32.	NSA	National Security Agency
AL1.1.33.	NTIS	National Technical Information Service
AL1.1.34.	OSD	Office of the Secretary of Defense
AL1.1.35.	PCAT	Personal Computer Access Tool
AL1.1.36.	PSA	Principal Staff Assistant
AL1.1.37.	REDIS	Reverse Engineering for Data Integration and Sharing
AL1.1.38.	SIDR	Secure Intelligence Data Repository
AL1.1.39.	SME	Subject Matter Expert

AL1.1.40.	SPARC	Standards Planning and Requirements Committee
AL1.1.41.	TAFIM	Technical Architecture Framework for Information Management
AL1.1.42.	WWW	World Wide Web
AL1.1.43.	1NF	First Normal Form
AL1.1.44.	2NF	Second Normal Form
AL1.1.45.	3NF	Third Normal Form

C1. CHAPTER 1

GENERAL INFORMATION

C1.1. INTRODUCTION

Standard data is the cornerstone of the information infrastructure that supports the Warfighter and the overall mission of the Department of Defense (DoD). Sharing information is critical to success on the battlefield and in the supporting functional areas. Standard data will enable DoD to perform its missions in an integrated, effective, and efficient manner.

C1.2. PURPOSE

C1.2.1. This Manual provides the procedures for developing, approving, implementing, and maintaining DoD data standards. A data standard provides the framework for how data will be formatted for implementation within an information system.

C1.2.2. The procedures contained in this document support the policies of DoD Data Administration as established by DoD Directive 8320.1 (reference (g)). These procedures are authorized as supplemental guidance to DoD 8320.1-M (reference (a)). Use of these procedures will improve the consistent and uniform identification and standardization of data.

C1.2.3. The context diagram shown in Figure C1-F1 presents the overall picture of the activities supporting the standardization of data within this Manual. The fundamental activities required to standardize DoD data requirements are listed in the node tree diagram in Figure C1-F2. This diagram was developed using the IDEF0 notation from FIPS PUB 183 (reference (e)). Throughout subsequent chapters of this Manual, detailed decompositions of this diagram will be displayed and described to enable users of this Manual to more clearly understand the interrelationships among the activities supporting the standardization of data.

C1.3. APPLICABILITY AND SCOPE

C1.3.1. This document applies to all DoD organizations under the conditions specified in DoD Directive 8320.1.

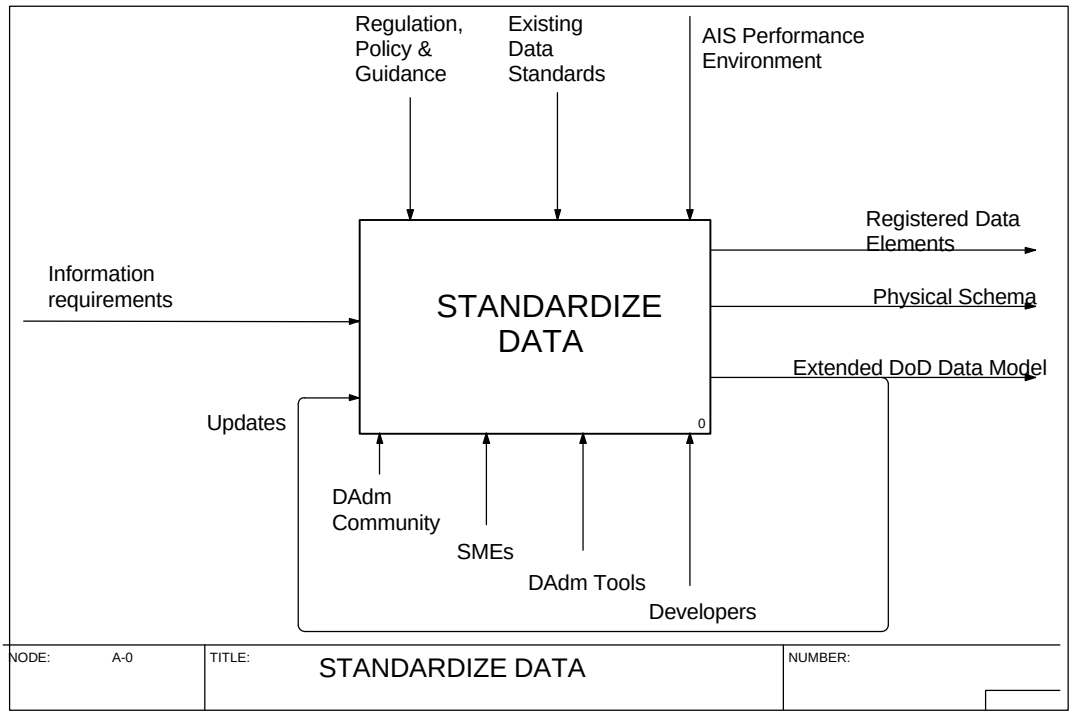


Figure C1-F1 Standardize Data

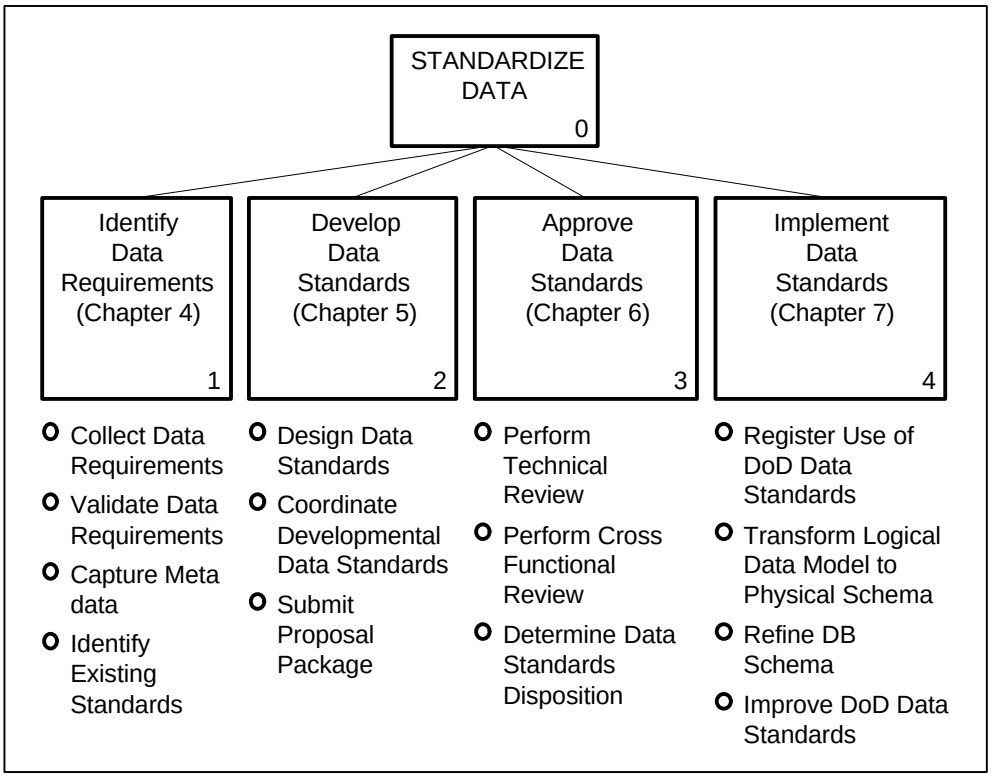


Figure C1-F2 Data Standardization Node Tree

C1.3.2. These guidelines apply to Information System (IS) components of weapon systems and DoD Automated Information System (AIS) development efforts, modification or modernization efforts affecting 30% or more lines of code. These guidelines also apply to system development efforts governed by the DoD Joint Technical Architecture (JTA). Deferments due to extenuating circumstances may be granted by the DoD Data Administrator based on an implementation plan that clearly describes a transition to the use of DoD standard data. IS components of weapon systems and AISs will be referred to jointly in this Manual as (ISs). A fully attributed data model will be assessed during Milestone Decision Point (MDP) I, Approval to Begin New Acquisition Program; an approved AIS data model will be assessed during MDP II, Approval to Enter Engineering and Manufacturing Development (reference (h)).

C1.3.3. To maximize data sharing across the DoD, data standardized in accordance with these procedures and migration systems data must be registered and approved in the DoD data dictionary. The DoD data dictionary is the authoritative source of DoD data standards and is the mechanism to be used in the data standardization approval process. See AP9. Appendix 9 for additional details.

C1.3.4. Classified data standards should follow the guidelines in this document but not be submitted for standardization. The capability to store classified data has been developed within the Secure Intelligence Data Repository (SIDR) (AP9. Appendix 9).

C1.3.5. Functional and Component level dictionaries and repository tools should not duplicate the DoD level of functionality. These tools may provide for internal requirements not supported by the DoD tools, and they may support the implementation of approved data standards.

C1.4. OBJECTIVES

C1.4.1. The objective of DoD data standardization is the use and reuse of data standards throughout the DoD in support of IS design and development; interoperability; data sharing; system integration; and business process improvements. Specific objectives are to:

C1.4.1.1. Develop and maintain a DoD Data Model (DDM) that depicts the DoD’s information requirements.

C1.4.1.2. Develop data standards from logical data models to promote interoperability among information systems, operational

forces, and the DoD functional areas in support of military missions throughout the DoD.

C1.4.1.3. Control data redundancy.

C1.4.1.4. Reduce the cost and time to develop, implement, and maintain systems.

C1.4.1.5. Enhance information system interoperability by reducing the requirements to translate and transform data.

C1.4.1.6. Provide for the uniform description and representation of data.

C1.4.1.7. Improve data integrity and accuracy.

C1.4.1.8. Document approved standard data in a single DoD data dictionary.

C1.4.1.9. Use applicable international, national, and Federal standards where appropriate.

C1.5. EXCEPTIONS TO PROCEDURES

Exceptions to the procedures established in this Manual will be considered on a case by case basis. Possible exceptions will be validated by the appropriate CDAd or FDAd and, if valid, will be forwarded to the DoD Data Administrator for resolution.

C2. CHAPTER 2

DATA STANDARDIZATION CONCEPTS

C2.1. INTRODUCTION

This chapter addresses the basic components of data standards (logical data models and meta-data) and describes the primary data standardization activities: identify data requirements, develop data standards, approve data standards, and implement data standards.

C2.2. BASIC COMPONENTS OF DATA STANDARDS

C2.2.1. Logical Data Models. All DoD data standards are based on an Entity Relationship Diagram (ERD) approach for the description of data needs. The ERD approach brings discipline to the description of data requirements.

C2.2.2.1. The logical data models developed using this approach must be in at least third normal form (3NF) to support the standardization of data. 3NF refers to an entity that is in second normal form and in which every non-key attribute is only dependent on the primary key. Refer to FIPS PUB 184, reference (b) for detailed information on developing a logical data model.

C2.2.2.2. Logical data models are created to support data requirements for DoD systems, functional areas, and DoD components. As logical data models are fully attributed, normalized, and validated by subject matter experts (SMEs) and system proponents, the models and supporting meta-data are submitted for the review, approval, and integration phases of data standardization.

C2.2.2.3. Logical data models submitted for review must be based on a version of the DoD Data Model (DDM) that is no more than one release old from the time of submission. The DDM is an integration of logical data models across multiple functional areas throughout the DoD. The DDM is published semiannually by the DoD Data Administrator (DoD DAd). It consists of a graphical representation of the data, based on the IDEF1X standard from reference (b). Detailed meta-data descriptions are found in the DoD data dictionary. Logical data models consist of the following components:

C2.2.2.3.1. Entities. Representations of real or abstract things (people, objects, places, events, ideas, combinations of things, etc.) that are recognized as the same type because they share the same characteristics and can participate in the same relationships (reference (b)).

C2.2.2.3.2. Attributes. Properties or characteristics that are common to some or all of the instances of an entity. An attribute represents the use of a domain in the context of an entity (reference (b)). In DoD terminology, attributes are also referred to as data elements.

C2.2.2.3.3. Relationships. Relationships are associations between two entities or between instances of the same entity (reference (b)).

C2.2.2. Meta-Data. Meta-data is "data about data" or the characteristics of an entity or attribute. Meta-data is stored in the DoD data dictionary. A description of meta-data for DoD data standards is provided in AP1. Appendix 1. Refer to the DoD data dictionary for the most current meta-data requirements.

C2.3. DATA STANDARDIZATION PHASES

Data standards evolve through the following standardization phases:

C2.3.1. Developmental. Entities and attributes (data elements) that have been created but have not been released by the originator for DoD standardization. Developmental data standards include both new data requirements and modifications to existing data standards as specified in C5. Chapter 5.

C2.3.2. Candidate. Entities and attributes that have been submitted for approval as DoD data standards as specified in C6. Chapter 6.

C2.3.3. Approved. Entities and attributes that have been coordinated through the standardization process and approved by the appropriate Functional Data Administrator (FDAd) as specified in C6. Chapter 6.

C2.3.4. Disapproved. Entities and attributes that have been coordinated through the standardization process and whose use has been disapproved as specified in C6. Chapter 6.

C2.3.5. Archived. Entities and attributes that were formerly approved, but are no longer needed to support the information needs of DoD as specified in C6. Chapter 6.

C2.4. DATA STANDARDIZATION ACTIVITIES

The activities addressed in this Manual include the identification, development, review, approval, implementation, and maintenance of data standards. Through these activities, sources of information are collected, modified, and reviewed, resulting in an expanded DDM and approved standard data. The primary data standardization activities are depicted in Figure C2-F1.

C2.4.1. Identify Data Requirements

C2.4.1.1. This activity results in the documentation of data requirements and associated meta-data, domain values, and authoritative sources. Data administrators should review all data requirements to be supported by an operational system. Current regulations must be considered in identifying the data requirements.

C2.4.1.2. Reuse applicable external (federal, national and international) data standards before creating DoD data standards. External data standards are those data standards that have been adopted by federal, national and international standards bodies such as the American National Standards Institute (ANSI), Federal Information Processing Standards (FIPS), International Organization for Standardization (ISO), and the North Atlantic Treaty Organization (NATO). The data administration community should review existing data standards to determine if they can support the data requirements. Modifications to existing DoD data standards to support requirements or the need to archive existing data standards should also be identified. Detailed procedures for this activity are provided in C4. Chapter 4.

C2.4.2. Develop Data Standards

This activity governs the development of new data requirements documented in the “Identify Data Requirements” activity. These requirements are represented in a logical data model to be proposed as an extension to the DDM. If a data standard is not found that meets the data requirement, then a new DoD data standard may be proposed. Modifications to DoD data standards or archiving of DoD data standards may also be proposed. Proposals for new and modified data standards are documented in the DoD data dictionary. A data model proposal package, described in C5. Chapter 5, is the vehicle for reviewing and approving proposed data standards.

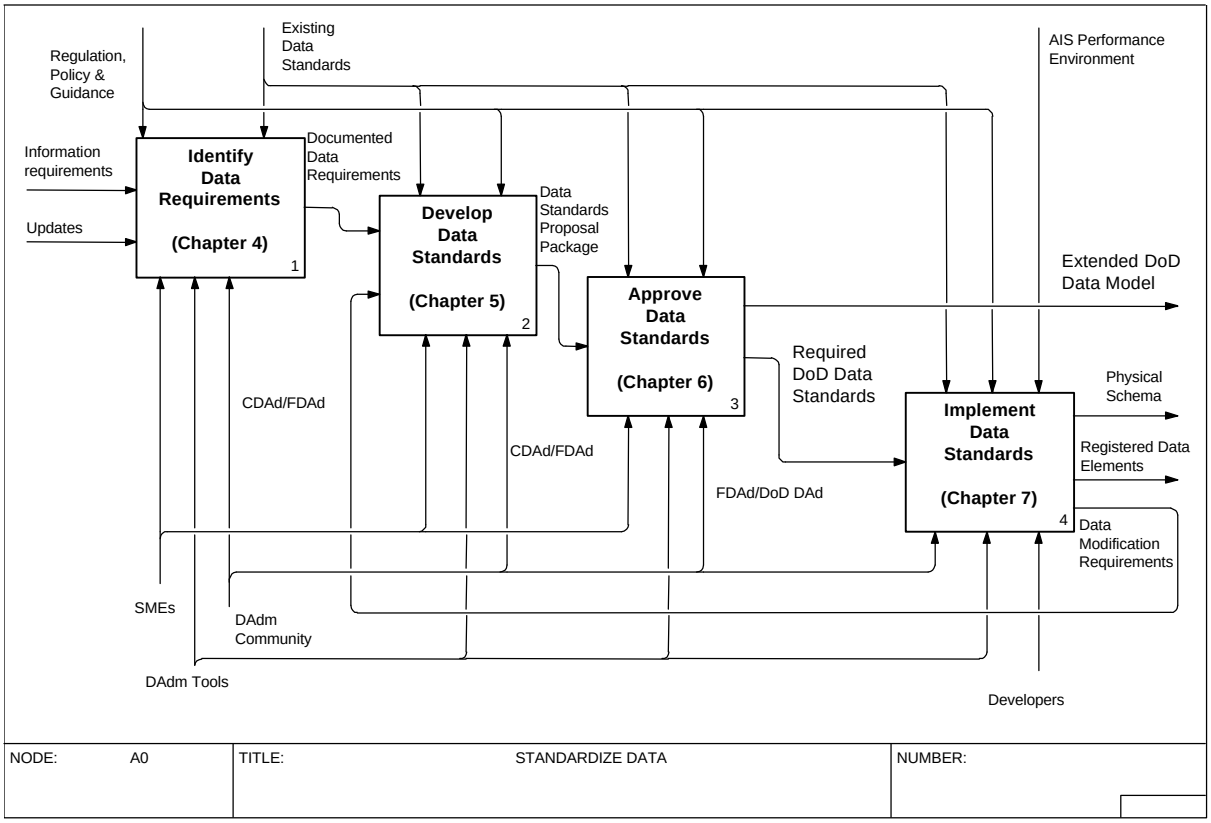


Figure C2-F1 Data Standardization Activities

C2.4.3. Approve Data Standards

In this activity, proposed data standards, modifications to existing data standards, and/or requests to archive existing data standards are reviewed for approval by the data administration community. When approved, the data standards will result in the expansion and/or modification of the DDM. Detailed procedures for the review, approval, disapproval, and resolution of proposed data standards are provided in C6. Chapter 6.

C2.4.4. Implement Data Standards

This activity addresses the implementation and improvement of approved data standards in DoD ISs. Approved data standards contained within the expanded DDM facilitate DoD IS modernization efforts. Detailed procedures for this activity are provided in C7. Chapter 7.

C3. CHAPTER 3

ROLES AND RESPONSIBILITIES

C3.1. INTRODUCTION

Expansion of the DDM and development of DoD data standards through functional area data modeling require participation across all functional communities. This chapter identifies the key participants and their roles and responsibilities in the DoD data standardization process. Additional DoD Data Administration responsibilities can be found in reference (a) and reference (g).

C3.2. PARTICIPANTS

C3.2.1. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I))

The ASD(C3I) is the designated Chief Information Officer (CIO) within the Department of Defense. The ASD(C3I) resolves issues for which a resolution can not be reached during the cross functional review. The ASD(C3I) has final authority on all issues.

C3.2.2. DoD Data Administrator (DoD DAd)

The DoD DAd develops and implements DoD procedures for data standardization. The DoD DAd is selected by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)). The DoD DAd responsibility has been delegated to the Defense Information Systems Agency by the ASD(C3I).

C3.2.3. Functional Data Administrator (FDAd)

FDAds manage and implement data administration within their functional areas. FDAds are designated by Office of the Secretary of Defense Principal Staff Assistants (OSD PSAs), and are assigned stewardship for data under their functional areas of responsibility as specified in reference (g).

C3.2.4. Component Data Administrator (CDAd)

CDAds represent the services, agencies, and the CINCs. CDAds have executive agent responsibilities over their operational systems and ensure standardization and implementation of data standards within ISs.

C3.2.5. Subject Matter Expert (SME)

SMEs are functional and technical experts within the Department of Defense who support the design, development, review, implementation and maintenance of DoD data standards.

C3.2.6. IS Functional Proponent

IS functional proponents provide data administration support for the implementation and establishment of DoD data standards.

C3.2.7. IS Program Manager

IS program managers provide for the configuration management of data and databases. Configuration management includes the use, reuse, establishment, and implementation of DoD data standards.

C3.3. ROLES AND RESPONSIBILITIES

C3.3.1. ASD(C3I)

The ASD(C3I) issues policy and guidance on DoD Data Administration, designates a DoD DAd, and resolves data issues that cannot be agreed upon by the DoD DAd, FDAds, CDAds and other SMEs.

C3.3.2. DoD DAd

C3.3.2.1. The DoD DAd supports the FDAds and CDAds in the development and submission of their data requirements. The DoD DAd is responsible for integrating logical data models from a DoD-wide perspective, based on DoD information requirements. This is accomplished by maintaining the DDM. The DoD DAd performs technical reviews of logical data models and meta-data, providing a technical disposition of data standards.

C3.3.2.2. Additional responsibilities include development of generic and external data standards, and periodic assessments of DoD data standards contained in the DoD data dictionary. Through the DoD data dictionary, the DoD DAd announces proposals for the archival of data standards.

C3.3.2.3. Unresolved issues that are presented after a cross functional review are forwarded to the DoD DAd for review and resolution.

C3.3.3. FDAd

C3.3.3.1. FDAds are responsible for coordinating and integrating all data requirements within their functional area.

FDAds will develop and publish a strategy for the development of data standards within their respective functional areas. The FDAds work directly with the DoD DAd.

C3.3.3.2. As a data steward, the FDAd is responsible for submitting data for standardization, functionally approving and/or disapproving data, and encouraging implementation of data standards. FDAds are responsible for notifying the registered users of standard data elements within their functional area when changes are proposed to those standards. Registered users are maintained in the DoD data dictionary. The FDAd is required to review and consider comments and recommendations presented as the result of cross functional reviews.

C3.3.3.3. Primary FDAd. Refers to the specific FDAd that receives a data standards proposal package from the package originator for approval as DoD standards. Also see C5. Chapter 5.

C3.3.3.4. Submitting FDAd. Refers to the specific FDAd that submits a data standards proposal package for approval as DoD standards. Also see C6. Chapter 6.

C3.3.3.5. Data Steward FDAd. Refers to the specific FDAd that is responsible for the approval of candidate data standards contained in a data standards proposal package under their stewardship. Also see C6. Chapter 6.

C3.3.4. CDAd

C3.3.4.1. CDAds provide oversight responsibilities to ensure the IS functional proponents and IS program managers are working to incorporate DoD data standards in the development or modification of ISs that support functional area(s).

C3.3.4.2. The CDAd provides expertise on the implementation and deployment of data standards. The CDAd provides expertise on registering application data to DoD data standards. The CDAd is responsible for reporting metrics on the use of DoD data standards in ISs under the administration and management of the service or agency.

C3.3.5. SME

SMEs bring detailed knowledge of data details, usage in ISs, and reporting requirements to collaborative sessions and functional reviews. SMEs support developers and reviewers of functional area data models with functional guidance and assistance for issue resolution. SMEs also support the integration of functional area data models into the DDM.

C3.3.6. IS Functional Proponent

The functional proponent for an IS is responsible for the identification of data requirements to be satisfied by an IS. Under situations where an IS is to satisfy joint requirements across the DoD services and agencies, the functional proponent is responsible for ensuring that the data needs are identified, reconciled, and described. Functional proponents are responsible for ensuring the establishment and reuse of data standards in IS design, development, modification, and improvement efforts. Responsibilities include the capture of metrics on the use of data standards in IS efforts and development of data models supporting the establishment and reuse of data standards.

C3.3.7. IS Program Manager

IS program managers are responsible for the configuration management of data and databases. Configuration management responsibilities extend to the implementation, deployment, and improvement of data standards. Responsibilities include the registration of application data to DoD data standards, capturing of metrics on the use of data standards in IS efforts and development of data models supporting the establishment and reuse of data standards.

C4. CHAPTER 4

IDENTIFY DATA REQUIREMENTS

C4.1. INTRODUCTION

This chapter addresses the collection and validation of data requirements, capture of meta-data requirements, and identification of existing data standards necessary to document DoD data requirements. This includes the requirements for modification or archiving of existing data standards. The activities are depicted in Figure C4-F1.

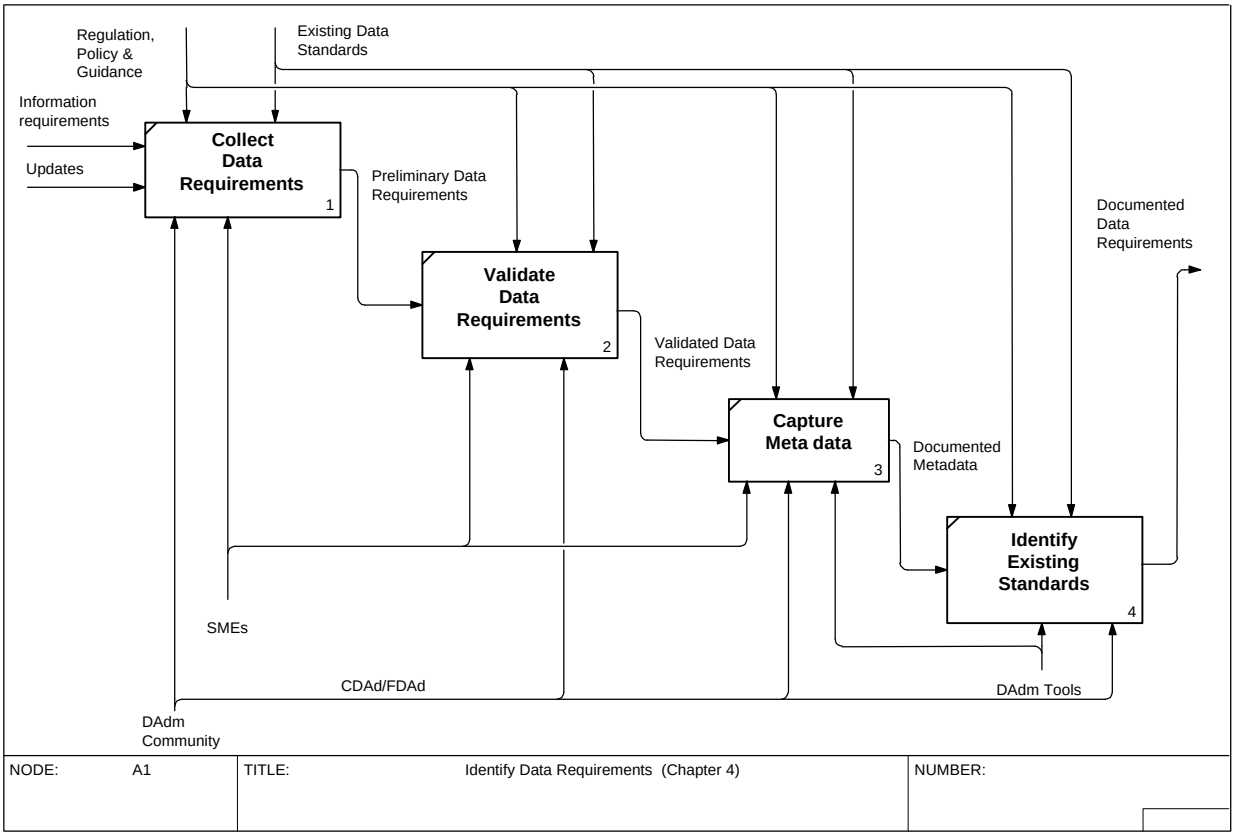


Figure C4-F1 Identify Data Requirements

C4.2. COLLECT DATA REQUIREMENTS

C4.2.1. Information necessary to support a specified mission requirement should be collected from appropriate sources. These information requirements may be collected from existing ISs; Operational Requirements Documents (ORDs); functional descriptions; and authoritative sources, such as policy and guidance. Information requirements may include a request to update (modify or archive) existing data standards. The

information requirements collected from these sources provide the preliminary data requirements.

C4.2.2. Reverse engineering is a technique that may be used as a method to collect information requirements from existing ISs. Detailed procedures are described in AP2. Appendix 2. This is an appropriate opportunity to associate existing application data elements to DoD data standards, by utilizing the matching or mapping techniques delineated in AP3. Appendix 3. Matching and mapping are used to aid developers in transitioning to the use of DoD data standards within ISs.

C4.2.3. The data standardization collection activities described in this Manual are exempt from licensing in accordance with paragraph E.4.d of DoD 8910.1-M (reference (f)).

C4.3. VALIDATE DATA REQUIREMENTS

Authoritative sources (official regulations, policy, guidance, public law, etc.) will be used as the basis for validating data requirements. Data administrators, subject matter experts, and information system program managers are responsible for the identification of appropriate sources for the data requirements. If a data requirement does not relate to an authoritative source list it should be removed from the preliminary data requirements. The authoritative source for each data requirement should be documented. The results of this activity are validated data requirements.

C4.4. CAPTURE META-DATA

The specific characteristics for each data requirement must be defined. Data requirements have definitive characteristics that quantify, identify, or describe a representational, administrative, or relational concept. Meta-data are characteristics of data such as definitions, domains, and units of measure. The specific set of meta-data required for data standardization is defined in AP1. Appendix 1. The meta-data for all unclassified DoD data standards will reside in the DoD data dictionary. The meta-data for all classified DoD data standards will reside in the Secure Intelligence Data Repository (SIDR) (AP9. Appendix 9).

C4.5. IDENTIFY EXISTING STANDARDS

C4.5.1. Meta-data provides the foundation for comparing the data requirements against existing data standards. The reuse of existing data standards will control redundancy and promote data shareability.

C4.5.2. Reuse applicable external (federal, national and international) data standards before creating or modifying a DoD data standard. FDAd's should be consulted to identify existing standards within their functional areas. The DoD data dictionary should also be used to locate adopted external and DoD data standards. Detailed procedures on reusing existing data standards are discussed in AP4. Appendix 4.

C4.5.3. External data standards may have to be modified to conform to the requirements of these procedures. Modifications may have to be made to the external data standard name, definition, or other characteristic to adapt the external data standard for DoD use. Detailed procedures on adopting external data standards for DoD use are contained in AP4. Appendix 4.

C5. CHAPTER 5

DEVELOP DATA STANDARDS

C5.1. INTRODUCTION

This chapter addresses the design and functional coordination of new data standards, modification to existing data standards, archiving of existing data standards, and the preparation and submittal of a data standards proposal package. The activities are depicted in Figure C5-F1.

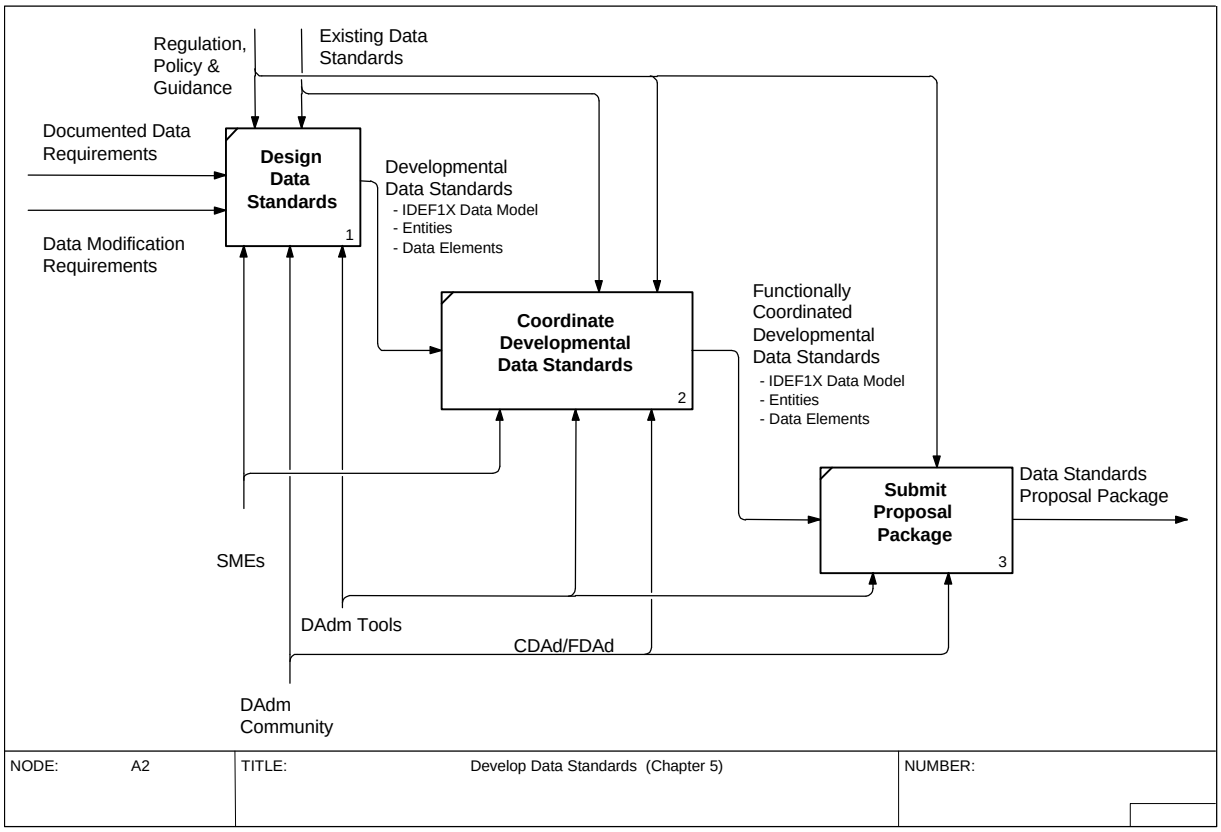


Figure C5-F1 Develop Data Standards

C5.2. DESIGN DATA STANDARDS

C5.2.1. All DoD data standards are based on an information engineering approach where documented data requirements are modeled (logical data model) to the Third Normal Form (3NF). An Entity Relationship Diagram (ERD) is a graphical representation of a logical data model. The design of developmental data standards includes the creation of an IDEF1X data model, entities and data elements. Developmental data standards include both new data requirements and modifications to existing data standards.

C5.2.2. Develop Data Model

C5.2.2.1. The first step in the design of developmental data standards is to model the documented data requirements. IDEF1X is the approved DoD standard for model presentation and the modeling notation that is used to expand and maintain the DDM. Data models developed in other than the IDEF1X method must be capable of conversion to IDEF1X syntax. Refer to AP2. Appendix 2 for procedures regarding reverse engineering of data models.

C5.2.2.2. A version of the DoD Data Model (DDM) no longer than one release old (approved and candidate data standards) must be used as the basis for the logical model. This ensures that relevant entities and attributes are incorporated into the logical data model where appropriate. Proposed modifications to approved entities, attributes and entity relationships should be incorporated into the logical data model. Through iterative steps the logical data model should be fully attributed and normalized to third normal form.

C5.2.2.3. Entities and attributes should be named and defined as described in AP5. Appendix 5. Relationship names between entities (business rules) are mandatory.

C5.2.2.4. Detailed procedures for developing IDEF1X data models are contained in reference (b). Additional guidance for developing logical data models for integration with the DDM is contained in AP6. Appendix 6.

C5.2.3. Document Developmental Entities and Data Elements

C5.2.3.1. The entities and attributes defined in the logical data model become the developmental entities and data elements in the DoD data dictionary. The originator will enter the developmental entities and data elements into the dictionary with their associated meta-data.

C5.2.3.2. Modifications to approved DoD data standards must also be entered into the DoD data dictionary. These modifications will be entered as a developmental version of the approved DoD data standard. If the modification is approved, the previously approved DoD data standard will be archived.

C5.2.3.3. The DoD data dictionary must be updated to reflect a request to archive an approved data standard. In this case, a version of the approved data standard is generated to reflect “Submit for Archive” status instead of “Developmental” status. Meta-data requirements are defined in AP1. Appendix 1. Refer to the DoD data dictionary for the most recent meta-data requirements and procedures for using the data dictionary.

C5.2.3.4. Any data element with a specific domain must have its complete set of domain values documented in the DoD data dictionary. All data elements using the class word “CODE” must have a specific domain.

C5.2.3.5. Any data elements using the class word “IDENTIFIER” and proposed as primary key attributes must represent “real world” identifiers and be unique across the DoD. The Authority Reference Text, cited for these IDENTIFIER data elements and documented in the DoD data dictionary, should contain the justification for the use of the identifier and the method for how it is created and maintained. If the Authority Reference Text does not provide this information, the method and/or plan for creating and maintaining the identifier should be documented in the DoD data dictionary in the data element Comment Text. (See AP1. Appendix 1 for the definition of the data element meta-data requirements, Authority Reference Text, and Comment Text.)

C5.3. COORDINATE DEVELOPMENTAL DATA STANDARDS

C5.3.1. A preliminary review shall be conducted within the functional community to coordinate the developmental data standards. This is an iterative process requiring the participation of the originator, SME(s), CDAd(s), and FDAd(s). For alternative data standardization development activities, refer to AP7. Appendix 7.

C5.3.2. Data standards originating in support of an OSD functional area requirement should be coordinated with the appropriate FDAd. Data standards originating within a Component or at the Component level shall be coordinated with the appropriate CDAds and FDAds.

C5.3.3. Prior to placing proposed modifications to approved DoD data standards into candidate status, the model originator will coordinate proposed changes with the affected IS program managers that have registered as users of the approved DoD data standards. This coordination will enable IS program managers to measure the impact of the proposed modifications on existing systems. Based on this impact assessment, the appropriate FDAd(s) will determine the disposition of the proposed modifications to the approved data standards.

C5.3.4. The participants are encouraged to discuss the developmental data standards with their functional and DoD counterparts. Appropriate FDAds shall conduct a preliminary review and provide appropriate response to the originator within 30 working days.

C5.3.5. This review ensures that:

C5.3.5.1. The data standards do not already exist.

C5.3.5.2. The developmental data standards comply with the guidance set forth in this Manual.

C5.3.5.3. The developmental data standards are in the DoD data dictionary.

C5.3.5.4. Functional data stewardship assignment for each proposed data standard has been assessed by the proposed FDAd steward.

C5.3.5.5. The logical data model is functionally integrated with the DDM.

C5.3.6. Any issues identified during the preliminary review must be resolved during this coordination.

C5.3.7. This activity results in functionally coordinated developmental data standards. The originator shall forward the developmental data standards to the primary FDAd in a data standards proposal package as specified in AP8. Appendix 8. Within 30 days of receiving the proposed data standards, the FDAd must provide to the originator and the DoD DAd a schedule for forwarding a completed proposal package to the DoD DAd. For details on the recommended tool set, refer to AP9. Appendix 9.

C5.4. SUBMIT PROPOSAL PACKAGE

This activity addresses the submission of a data standards proposal package for approval as DoD standards. The FDAd will propose the functionally coordinated developmental data standards as an extension or update to the DDM. Detailed procedures for assembling and submitting the proposal package are contained in AP8. Appendix 8.

C6. CHAPTER 6

APPROVE DATA STANDARDS

C6.1. INTRODUCTION

This chapter addresses the technical and cross functional review and approval of data standards. It includes the modification or archiving of existing data standards. These activities are depicted in Figure C6-F1.

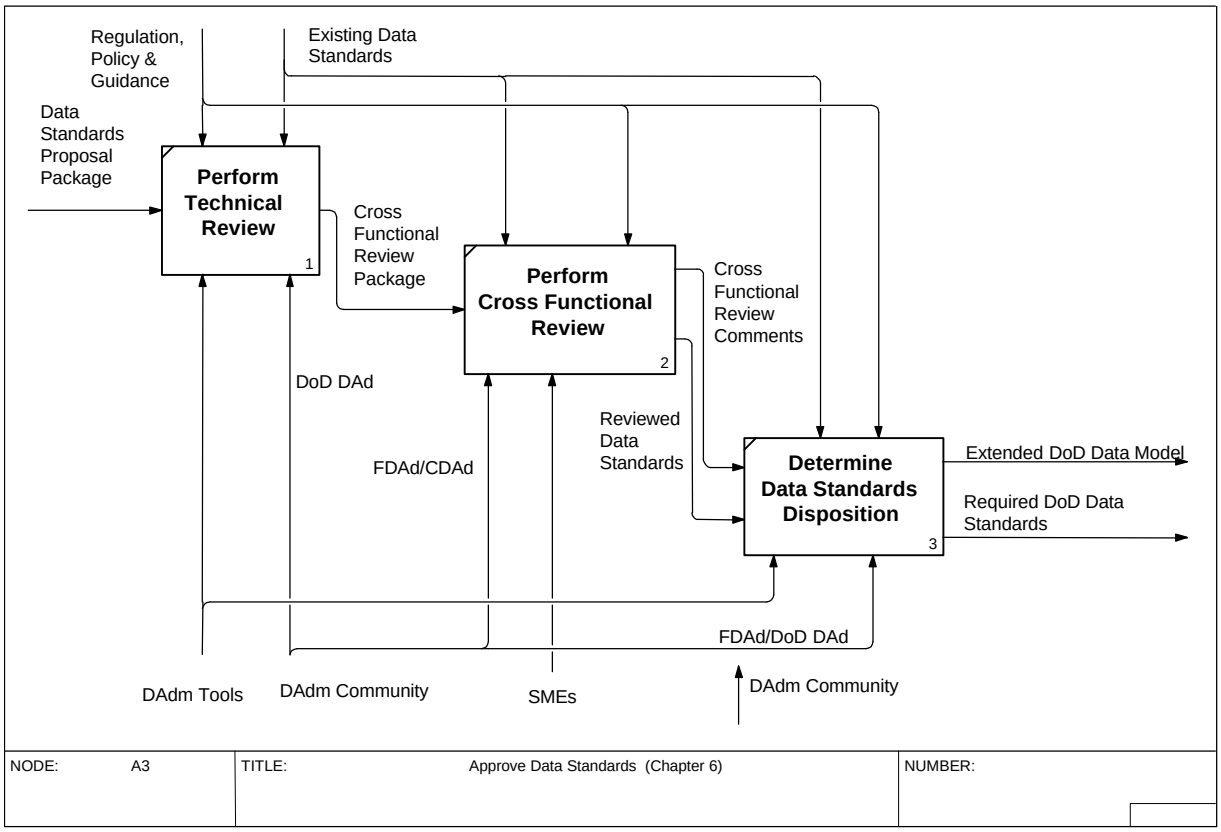


Figure C6-F1 Approve Data Standards

C6.2. PERFORM TECHNICAL REVIEW

C6.2.1. When the DoD DAd receives the proposal package from the FDAd, it is validated as described in AP8. Appendix 8. If the package is incomplete, the DoD DAd will coordinate with the submitting FDAd to obtain the missing information. Once it is determined the package is complete, notification will be made to the submitting FDAd and a technical review will be performed by the DoD DAd. Results of this technical review will be provided to the proposal package creator and submitting FDAd within 20 working days.

C6.2.2. The developmental data standards are technically reviewed to ensure that they conform to requirements established in this Manual. This includes an impact analysis of the proposed logical data model and the DDM for integration purposes. The DoD DAd may request an instance table to better understand the data requirement being proposed. Instance table examples are depicted in Figures C6-F2 and C6-F3.

PERSON Table (abbreviated)			
PERSON identifier (KEY)	**PERSON birth date**	**PERSON eye color code**	**PERSON usual weight**
555-82-2256	19660203	BL *(blue)*	185
695-44-2635	19690203	HZ *(hazel)*	125
123-45-6789	19551225	BR *(brown)*	210

Figure C6-F2 PERSON Instance Table Example

C6.2.3. The attribute PERSON identifier has migrated from PERSON to PERSON-NAME; the other two key attributes, PERSON-NAME date and PERSON-NAME category code further identify the PERSON-NAME text attribute. This accommodates name changes, title changes, etc. for a particular person (identified by PERSON identifier).

PERSON-NAME Table			
PERSON identifier (KEY migrated from PERSON table)	**PERSON-NAME date (KEY)**	**PERSON-NAME category code (F|M|S|C|T)(key)**	**PERSON-NAME text**
123-45-6789	19551225	F *(first name)*	Nicholas
123-45-6789	19551225	S *(surname)*	Jones
123-45-6789	19551225	M *(middle name)*	Frederick
695-44-2635	19890205	S *(surname)*	Richardson
123-45-6789	19551225	T *(honorary title)*	Mister
123-45-6789	19551225	C *(cadency)*	Junior

Figure C6-F3 PERSON-NAME Instance Table Example

C6.2.4. The technical review achieves the following:

C6.2.4.1. Ensures that the developmental data standards do not conflict with any existing candidate or approved data standards.

C6.2.4.2. Validates and integrates the proposed data standards with the current working version of the DDM.

C6.2.4.3. Ensures all entity and attribute meta-data information is complete and conforms to the requirements set forth in this manual. (See AP1. Appendix 1 and AP5. Appendix 5.)

C6.2.4.4. Ensures that IDEF1X model development and representation guidelines specified in AP5. Appendix 5 and reference (b) are adhered to.

C6.2.4.5. Verifies cardinality and relationship names.

C6.2.4.6. Verifies functional stewardship.

C6.2.5. The DoD DAd will coordinate with the FDAd to resolve technical and data stewardship assignment issues raised during the review. Once technical issues are resolved, the data standards are modified by the creator. The DoD DAd then prepares a cross functional review package and coordinates with the FDAd to promote the developmental data standards to candidate status in the DoD data dictionary. The FDAd and/or DoD DAd will promote the developmental data into candidate status. The cross functional review package contains the following:

C6.2.5.1. An integrated view of the proposed logical data model with the DDM.

C6.2.5.2. A list of the candidate entities and data elements.

C6.2.5.3. As applicable, a description of proposed modifications to existing data standards.

C6.2.5.4. As applicable, a description of archival requests of existing data standards.

C6.2.5.5. A cover letter containing the following information:

C6.2.5.5.1. Proposal package tracking number.

C6.2.5.5.2. DoD DAd point of contact information.

C6.2.5.5.3. Submitting FDAd information.

C6.2.5.5.4. Comment and recommendation suspense date.

C6.2.6. The cross functional review package is distributed to the data administration community for review. This distribution may be accomplished via fax, E-mail or other media.

C6.3. PERFORM CROSS FUNCTIONAL REVIEW

C6.3.1. The formal cross functional review ensures that the candidate data standards are represented uniformly with a DoD perspective. This review provides all DoD FDAds and CDAds the opportunity to review proposed extensions to the DDM. The cross

functional review period is 20 workdays. The review period begins on the first full day after notification is sent out. The cross functional review accomplishes the following:

C6.3.1.1. Ensures the candidate entities and data elements and required meta-data are clear, meaningful and consistent with cross functional area mission, objectives and information requirements.

C6.3.1.2. Validates that the candidate entities and data elements are represented uniformly with a DoD perspective so that they can be interpreted consistently.

C6.3.1.3. Validates that the entity relationships accurately reflect business rules that are implemented uniformly with a DoD perspective.

C6.3.1.4. Validates the requirement for the data standards within the framework of the DDM.

C6.3.1.5. Provides the functional community with the opportunity to review proposals for archived data and determine the impact the archival will have on current implementation.

C6.3.1.6. Ensures component unique data requirements are represented using as general terminology as possible. (non Service specific)

C6.3.2. Non-concurrence on a candidate data standard shall be based on an operational data requirement supported by both:

C6.3.2.1. A full justification including documentation (source regulations, mission statements, official policy, DoD Directives, laws, etc.) and where applicable, the estimated implementation costs and/or mission impact to support the disapproval.

C6.3.2.2. One or more technically and functionally compliant recommended alternatives with the estimated costs for implementation where applicable.

C6.3.2.3. Comments and or recommendations may not be accepted if they do not meet the criteria or if they are sent after the allotted review period as specified in the cover letter.

C6.3.3. This activity results in functionally reviewed data standards and the documentation of comments and recommendations generated from the cross functional review. Reviewing activities will forward their comments and recommendations to the submitting FDAd, data steward FDAds, and the DoD DAd in electronic copy

format (ASCII). The proposal package tracking number must be included with the comments.

C6.4. DETERMINE DATA STANDARDS DISPOSITION

C6.4.1. This activity describes the actions to be taken by the data steward FDAds and the DoD DAd on the candidate data standards as a result of the comments and recommendations received during the cross functional review. Final disposition is conducted within 10 workdays after completion of the cross functional review.

C6.4.2. The data steward FDAds and the DoD DAd evaluate the comments. The FDAd will determine the forum to obtain consensus on the data standards. The DoD DAd will assist the FDAd in determining the appropriate participants in the resolution process.

C6.4.3. The data steward FDAds and DoD DAd will ensure modifications are made to the DDM, entities and data elements based on comment resolution. The FDAd will ensure their respective logical data model is updated accordingly.

C6.4.4 Based upon the above evaluation, the data standards will either be approved, archived, disapproved, or forwarded for resolution.

C6.4.4.1. Approved. The data steward FDAds and the DoD DAd will change the candidate entities and data elements in the DoD data dictionary to “approved”. The FDAd provides functional approval and the DoD DAd provides technical approval.

C6.4.4.2. Approval of Generic Elements. The data steward for generic elements is the DoD DAd, who will make the approval decision. The approval of new generic elements shall be based on the FDAd recommendations and the following:

C6.4.4.2.1. The analysis of existing data elements to ensure that an existing class cannot be modified to include the new category.

C6.4.4.2.2. Extension of the DDM to ensure that data elements will be created to fit into this new class.

C6.4.4.2.3. Requirements to manage a new class of data for which standard rules are required.

C6.4.4.2.4. The DoD DAd will update the DoD data dictionary accordingly upon the approval decision.

C6.4.4.3. Archived. Archival of data standards can occur in the following ways:

C6.4.4.3.1. Approval of modifications to existing data standards (entities, data elements and associated relationships). This results in the archival of the previously approved version.

C6.4.4.3.2. Approval of request to archive an existing data standard (entities, data elements and associated relationships). This results in an "archived" data standard. A historical file will be maintained for archived data.

C6.4.4.4. Disapproved. The data steward FDAd and the DoD DAd will change the candidate entity(s) and data element(s) in the DoD data dictionary to "disapproved".

C6.4.4.5. Forwarded for Resolution. Documented functional issues not resolved by the DoD DAd and data steward FDAds will be coordinated with the applicable PSAs and forwarded to the Director, Defense Information Systems Agency for final resolution.

C6.4.5. The submitting FDAd will ensure that data stewards and data stakeholders provide appropriate written disposition on each comment received from the cross functional review. The proposal package FDAd will distribute these written dispositions to all data stewards and the DoD DAd. Upon final disposition, the DoD DAd will update the DDM accordingly.

C6.4.6. The principal outputs of the "Approve Data Standards" activity are:

C6.4.6.1. An extended DDM which has been revised by updates to DoD data standards (approved, archived, and disapproved standards);

C6.4.6.2. DoD data standards required for system development or modernization efforts.

C6.5. PERIODIC REVIEW OF DATA STANDARDS

C6.5.1. On a periodic basis, the FDAds will review all data standards that have not been approved and have remained static in the DoD data dictionary for longer than 30 days. The FDAd will take appropriate disposition on these data standards.

C6.5.2. The DoD DAd will run periodic reports on these data standards to assist the FDAds in determining appropriate disposition. Emphasis will be placed on the implementation of DoD data standards within information systems. DoD data

standards that do not have information systems registered against them will be reported to the appropriate FDAd.

C6.5.3. Developmental and candidate data standards that have not been approved and have remained static for longer than one year with no revisions or modifications, will be removed from the DoD data dictionary and users notified.

C7. CHAPTER 7

IMPLEMENT DATA STANDARDS

C7.1. INTRODUCTION

This chapter addresses several data standards implementation activities. The chapter is an overview of these activities since each implementation will be unique in technical design and data requirements. Implementation of DoD data standards contained in the DoD Data Model (DDM) shall be interpreted to mean that the DDM will serve as the logical database schema defining the names, representations, and relations of data within DoD systems. System developers comply by using this database schema as the basis for their own physical database schemas. Developers of new and existing systems shall maintain traceability between their physical database schema and the DDM by registering the use of data standards in the DDDS.

C7.2. GENERAL SYSTEM CONSIDERATIONS

C7.2.1. DoD maintains two synchronized tools for the storage and configuration management of DoD data standards. The first tool, called the DDM database, is a relational database used to store and maintain the DDM. It holds the IDEF1X representation of the DDM and contains entities, attributes, and entity relationships (business rules).

C7.2.2. The second tool is the Defense Data Dictionary System (DDDS). The DDDS is used to store and maintain information about DoD data standards. It contains standard data and its associated meta-data. For example, the DDDS contains the following, as appropriate, for each approved standard data element: entity, class word, data element name, data element definition, access name, data type, maximum field length, low range, high range, domain values, and domain value definitions.

C7.2.3. The DDM and the DDDS contain all the information necessary to create a data dictionary for an IS. Information in these tools can be used to develop database design specifications that can be converted to specific Database Management Systems (DBMS) Data Definition Languages (DDL). Portions of the model can be selected to support specific functions or applications.

C7.2.4. Activities relevant to the implementation of standards: register use of DoD data standards, transform logical data model to physical schema, refine database schema, and improve DoD data standards, are depicted in Figure C7-F1.

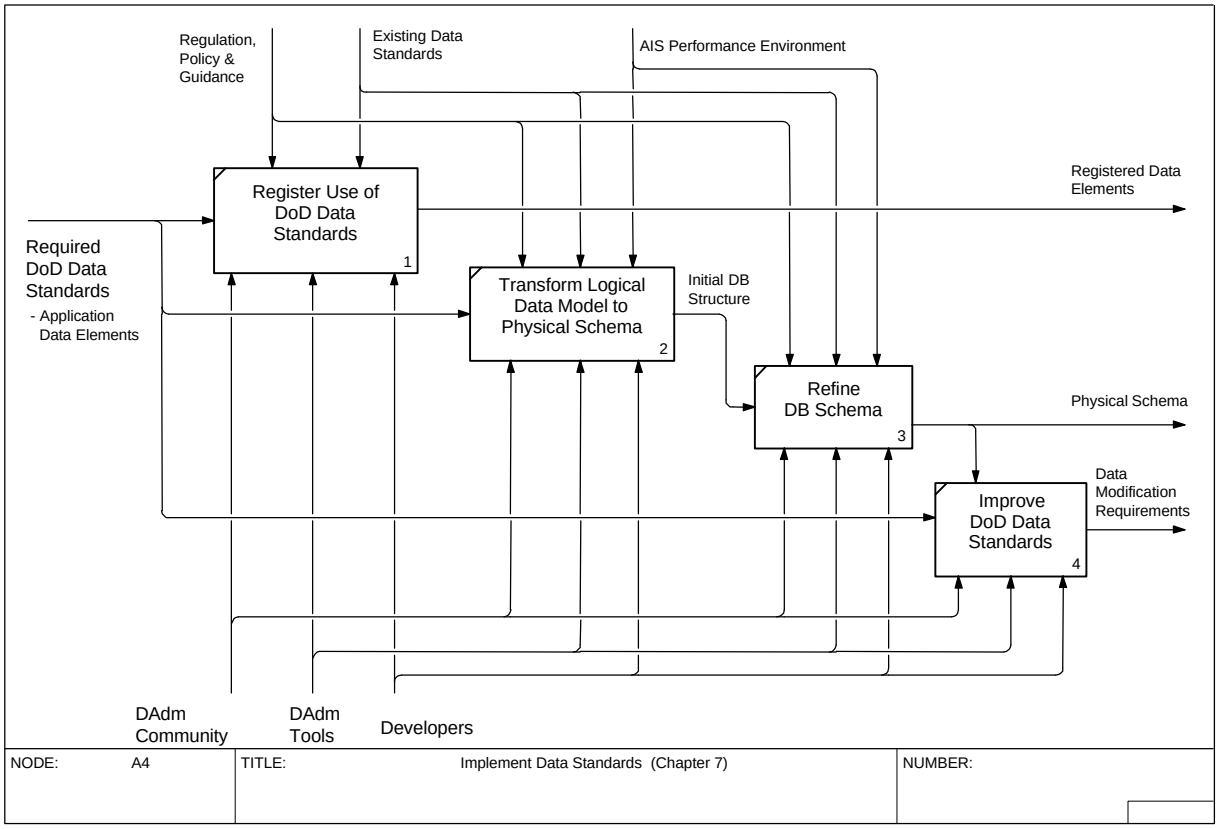


Figure C7-F1 Implement Data Standards

C7.3. REGISTER USE OF DoD DATA STANDARDS

C7.3.1. In using DoD data standards, implementers should be aware that DoD policy on registering the use of DoD data standards applies to both IS modernization efforts and modifications of existing ISs. This consists of DoD system modernization efforts authorized by Congressional mandate and/or under the Major Automated Information System Review Council (MAISRC) guidelines. Registering the use of DoD data standards is accomplished by associating a specific Defense Integration Support Tools (DIST) application with DoD standard data elements contained in the DDDS. The specific function in the DDDS is referred to as "Associating Applications With Standard Data Elements."

C7.3.2. DoD migration systems should use the matching and mapping guidelines delineated in AP3. Appendix 3 to facilitate the transition to DoD data standards in conjunction with changes in the underlying data structures that support these systems. Matching application data elements to DoD standard data elements is considered as using DoD data standards. Mapping application

data elements to DoD standard data elements is not considered as using DoD data standards.

C7.4. TRANSFORM LOGICAL DATA MODEL TO PHYSICAL SCHEMA

The IDEF1X logical data model developed and approved as specified in C4. Chapter 4, C5. Chapter 5, and C6. Chapter 6 can be transformed into an initial physical schema. This schema is then used to guide the development of a physical database. There are several actions that should be taken to transform DDM entities, relationships, and attributes into physical equivalents:

C7.4.1. DDM Entity and Attribute Conversion

C7.4.1.1. Transform the entity label from the DDM into a physical table name. Following Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS) (reference (i)) rules, table names should be less than or equal to 26 characters. Generally, table names should use the entity access names which utilize generally accepted acronyms (e.g., ORG, CIV), and be as short as possible to facilitate their use in DoD ISs. Entity access names can be obtained from the DoD data dictionary.

C7.4.1.2. The physical equivalent to the attribute name from the DDDS is the data element access name. Data item (column) names should be less than or equal to 18 characters.

C7.4.2. Data Type Selection

Physical equivalents to the data standards contained in the DDM require selection of appropriate data types based on the target physical database. Figure C7-F2 shows equivalent DDDS, SQL, SYBASE, and ORACLE data types. Factors affecting selection of data types include:

C7.4.2.1. Methods used by Commercial off-the-shelf (COTS) DBMS to implement character string -data types: CHAR, VARCHAR2, and LONG. Importantly, the use of each of these data types may be constrained by a maximum field length. For example, the data type CHAR can be no longer than 255 characters; VARCHAR2 can be no longer than 2000 characters; LONG holds as much as 2 gigabytes of data. In selecting an appropriate application data type, implementers are advised to look at the maximum character count quantity (i.e., Field Length) for the data item.

C7.4.2.2. Class word specified for the standard data element. Qualitative class words (e.g., Code, Identifier, Name, text) are typically implemented by one of the character string data types: CHAR, VARCHAR2, LONG. Special attention should be paid to the

use of the class word identifier. To preclude data type transformations in situations where mathematical computations are required, it is recommended that the SQL data type INTEGER and/or equivalent DBMS data type be used.

DDDS Data Types	SQL Data Types	Sybase Data Types	ORACLE Data Types
Character-String	CHAR(n) CHAR VARYING(n)	CHAR(n) VARCHAR(n) TEXT(n)	CHAR(n) VARCHAR2(n) LONG
Integer	INTEGER SMALLINT	INT SMALLINT	NUMBER
Fixed-Point	NUMERIC(p,s) DECIMAL(p,s)	NUMERIC(p,s) DECIMAL(p,s)	NUMBER(p,s)
Floating-Point	FLOAT(b) DOUBLE PRECISION REAL	FLOAT(b) DOUBLE PRECISION REAL	NUMBER FLOAT(b)
Bit-String		IMAGE	RAW(n) LONG RAW

Figure C7-F2 DDDS Data Types and Equivalents

C7.4.2.3. Data elements using quantitative class words. The following quantitative class words are typically implemented under ORACLE with the data type NUMBER: Amount, Angle, Area, Dimension, Mass, Quantity, Rate, Temperature, Volume, and Weight. Special attention should be given to both precision and scale in using the data type.

C7.4.2.4. Data elements using the quantitative class words, Date and Time. Implementers should be aware that COTS DBMS offer DATE as a data type to handle both date and time. In situations where the turn of the century data manipulation problem (i.e., year 2000 issue) can be handled by the use of the DATE data type, it should be used. In data interchange situations, a date attribute is a character string with the following format: YYYYMMDD; a time attribute is a character string with the format: HH:MM:SS.

C7.4.2.5. Low range specification for a standard data element. In the DDDS, for example, the low range for a standard data element may be -999.99 with the maximum character count quantity documented at 7 to account for the negative sign and the decimal point. Many COTS DBMSs handle both signed data and the placement of the decimal point through the use of precision and scale variables. Under SQL compliant databases the following specification is the same as -999.99: NUMBER(5,2).

C7.4.3. Other Factors

Physical implementation will require the capture of the appropriate field length for each data item. This information is carried in the DDDS as the maximum character count quantity. For quantitative attributes, the physical implementation should capture the allowable low range and high range values. For qualitative attributes, the physical implementation should use all or a subset of approved domain values and domain value definitions.

C7.4.4. Practical Application of Transformation Rules

C7.4.4.1. Figure C7-F3 depicts these transformation rules using the logical model for the storage and maintenance of Federal Information Processing Standard 10-4 (FIPS 10-4) (reference (j)) country codes.

LOGICAL MODEL

COUNTRY

COUNTRY CODE
COUNTRY NAME COUNTRY ABBREVIATED NAME COUNTRY SCOPE NOTE TEXT

PHYSICAL INSTANCE TABLE

TABLE NAME: COUNTRY

COLUMN NAME	CY_CD	CY_NM	CY_ABBRD_NM
KEY TYPE	PK		
NULLS/UNIQUE	NN,U	NN	
FK REF Table			
FK REF NAME			
DATA TYPE	CHAR	VAR CHAR 2	CHAR
MAX. FIELD LENGTH	2	50	5
SAMPLE DATA	AF	AFGHANISTAN	
	AS	AUSTRALIA	
	BF	BAHAMAS, THE	
	BK	BOSNIA AND HERZEGOVINA	
	GQ	GUAM	
	HR	CROATIA	
	MK	MACEDONIA	
	SR	SERBIA	
	US	UNITED STATES	
	ZI	ZIMBABWE	

Figure C7-F3 Transition from Logical Data Model to Physical Table

C7.4.4.2. The entity COUNTRY becomes the table COUNTRY. The data items in the table (column names) are the access names from the DDDS. The data types (e.g., CHAR, VARCHAR2) were selected based on the information on data types. The field length for each data item was taken from the DDDS as the maximum character count quantity.

C7.4.4.3. The implementation of the data standards requires that: physical tables be created in the appropriate Data Definition Language (DDL), the country table be populated with the standard domain values and domain value definitions. These two activities are illustrated in Figure C7-F4. This figure shows the load script that has been written to populate the country table.

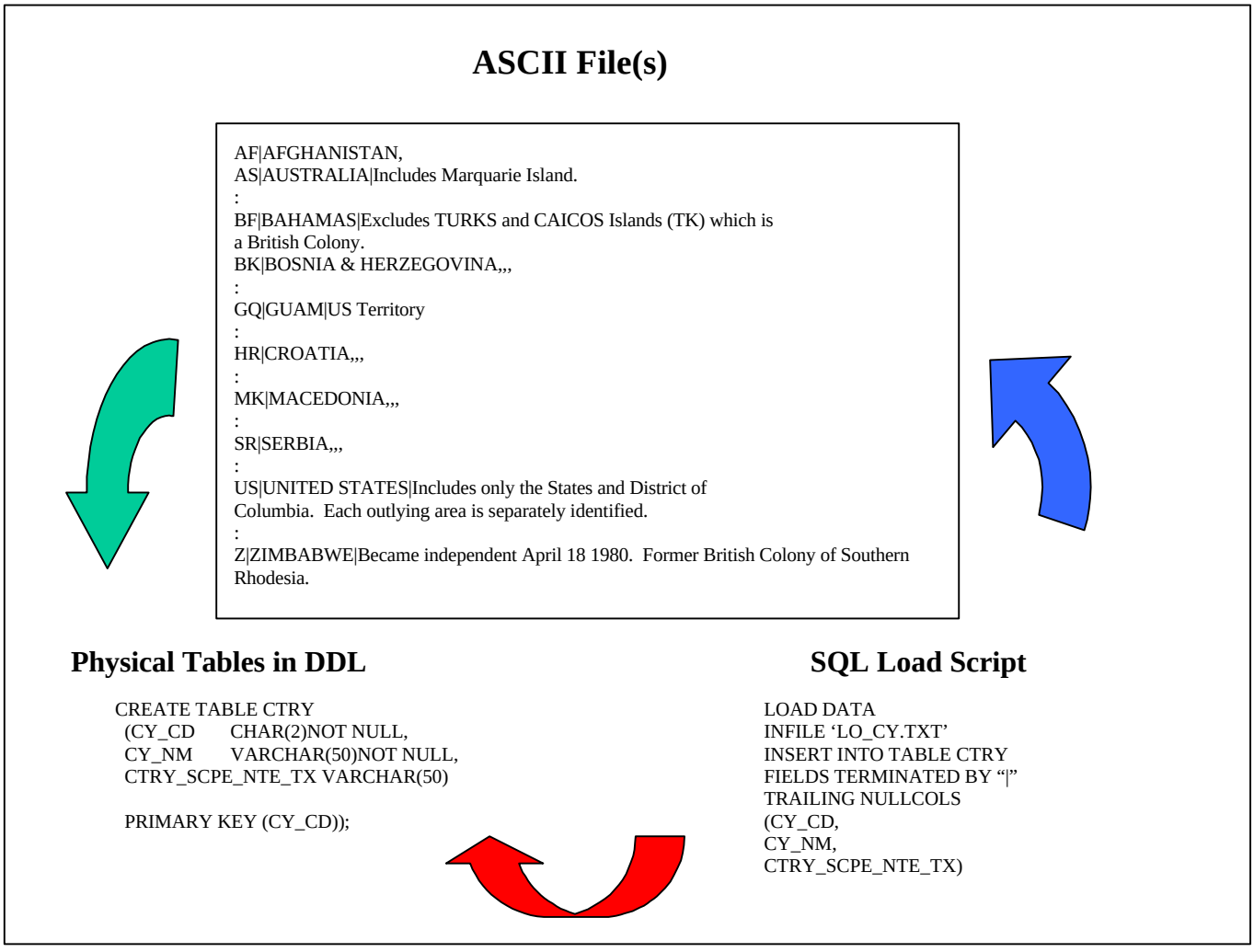


Figure C7-F4 Extraction and Load of Standard Domain Values and Domain Value Definitions

C7.4.4.4. The implementation of the data is not quite complete. Additionally, implementers must analyze the impact that the transition to the data standard will have on the operational system. Several types of impacts are anticipated:

C7.4.4.4.1. An existing country code table may have to be dropped from an IS. This will require an analysis of methods and procedures on how to effectively drop the table without disrupting data integrity.

C7.4.4.4.2. Domain values and domain value definitions may be added to an existing country code table. This approach provides for an incremental adoption of the standard and may allow time to complete the transition to approved standards.

C7.4.4.4.3. Existing documentation on an operational IS may have to be updated. It is recommended that updates be made on a case-by-case basis to only essential documents. Typically these are user manuals, maintenance manuals, and database specifications. The most effective way to ease the update is through the use of help screens, on-line notifications, and change pages to electronic and paper documents.

C7.5. REFINE DATABASE (DB) SCHEMA

C7.5.1. The example provided on the implementation of a standard country code table is used for explanatory purposes only. The individual IS performance environment will be used as the basis for the refinement of the initial physical DB schema.

C7.5.2. Additional factors to be considered in implementing data standards include: table consolidations, DBMS performance, decision support (retrieval) optimization, time stamped data, transaction processing (insertion and update) optimization, data security and MLS requirements, data distribution and replication, data fusion in the Command and Control (C2) tactical and intelligence functions, and alternate ways to implement concept and/or logical data models.

C7.6. IMPROVE DoD DATA STANDARDS

C7.6.1. The implementation of data standards is the final validation of approved DoD data standards. To support the DoD IS interoperability goals, it is imperative that the DDM and the DDDS reflect data standards that are both implemented and operational. To fulfill this requirement, the implementation of data standards includes the modification and improvement of data standards. These modifications and improvements may be as simple as adding a domain value and domain value definition to an approved list. They may be as simple as changing an allowable field length (maximum character count quantity). They may be

entire replacements for an independent entity view or subject area.

C7.6.2. Modifications and improvements may also include the identification of data standards that are no longer implemented in any IS, and therefore should be archived. Whatever the case, the modification and improvement of DoD data standards requires the participation of Central Design Activities, system developers, and implementers. This activity provides for the identification, classification, and analysis of potential improvements to DoD data standards that are driven by the implementation and deployment of data standards.

C7.6.3. Once modifications to existing standards have been identified and proposed (as discussed in C4. Chapter 4, C5. Chapter 5, and C6. Chapter 6), it is the responsibility of the organizations assigned to develop or maintain ISs to determine the impact of the proposed modifications. Comments and concerns regarding the proposed modifications should be addressed through the cross functional review process, as detailed in C6. Chapter 6. If proposed modifications are approved the previous version of the data standard is archived. Users of the archived data standard must, within a 12 month period, either implement the new version of the data standard or submit to the appropriate FDAd and DoD DAd a plan for implementing the new version.

AP.1 APPENDIX 1

META-DATA REQUIREMENTS

The meta-data requirements for DoD data standards are listed in the following tables. Meta-data are annotated as “M,” "C," or "O," in the “OBLIGATION” column as follows:

M = Mandatory - always required
C = Conditional - required to be present under certain specified conditions
O = Optional - allowed but not required

Meta-data requirements are documented in the DoD Data Dictionary.

AP1.1. ENTITY META-DATA

ATTRIBUTE	OBLIGATION	ATTRIBUTE DEFINITION
Entity Name	M	The label of an entity; must be a noun or noun phrase with the entire phrase connected by hyphens; must accurately reflect the characteristics (attributes) of itself, especially its domain.
Access Name	M	An abbreviated name representing a specific entity.
Definition Text	M	The narrative description of what an entity is.
Comment Text	O	Additional narrative description of an entity.
Version Identifier	M	Used for configuration management of the object; based on modifications of approved standards; system generated based on actions taken by the appropriate data administrators.
Counter Identifier	M	The “record number” within the DDDS (system generated); unique to the category of data standard.
Status Code	M	The stage within the approval cycle; system generated based on actions taken by the appropriate data administrators.
Functional Area Identifier	M	An indicator of the functional area of responsibility within the Department of Defense to which an entity or data element belongs. Can be selected from a list in the system. Areas may be added and/or modified based on customer request supporting changes to missions of the DoD.

Steward Name	M	Dependent on functional area; a steward is responsible for certain functional areas and the validity of data contained in standard data elements within the functional area. This is system generated based on the functional area identifier.
Using Model Name	M	The association of an entity with one or more data models.

AP1.2. DATA ELEMENT META-DATA

ATTRIBUTE	OBLIGATION	ATTRIBUTE DEFINITION
Standard Data Element Name	**M**	The label of an attribute, comprised of a minimum of an entity and generic element; may contain property modifier(s) providing additional descriptions; may utilize generic data; must be a noun or noun phrase and accurately reflect the characteristics (meta-data) of the attribute, especially domains.
Counter Identifier	**M**	The "record number" within the DDDS (system generated); unique within a category of data standard.
Status Code	**M**	The stage within the approval cycle; DDDS generated based on actions taken by the appropriate data administrators.
Service and/or Agency Component Code	**M**	The organization to which the creator is assigned (system generated).
Short Access Name	**M**	A short abbreviated name representing a specific data element. An access name is used to reference a data element in a database and must conform to the syntactical requirements of the database management system (DBMS) or programming language of the application in which a data element is used. The maximum length for an access name is 18 characters. The system will generate an access name if one is not provided.

Long Access Name	**O**	A long abbreviated name representing a specific data element. This name is used to reference a data element in a database and must conform to the syntactical requirements of the database management system (DBMS) or programming language of the application in which a data element is used. The maximum length for a functional abbreviation access name is 30 characters.
Data Type Name	**M**	The name of the way domain values are stored in a database. The generic data elements with class words having a data type of "integer" will be modified with a comment (comment text field) as follows: Data element using the data type "integer" should fit into a 32 bit representation. The high range value of a signed integer is limited to "2.1 billion" (in the range -2^{31} to $2^{31}-1$); data requirements of greater values should use the data types "floating point" or "fixed point".
SQL Data Type Name	**O**	The SQL name of the way domain values are stored in a database.
Functional Area Identifier	**M**	An indicator of the functional area of responsibility within the DoD to which an entity or data element belongs. Can be selected from a list in the DDDS. Areas may be added and/or modified based on customer request supporting changes to missions of the DoD.
Security Category	**M**	A classification assigned to the data element domain value identifiers stored in some physical media to show the level of protection required to prevent their disclosure.
Maximum Character Count Quantity	**M**	The field length of the data; it should be large enough to accommodate all requirements, yet precise enough to allow for accuracy.
Timeliness Identifier	**O**	A description of the frequency of updates to the domain, this information will inform implementers and/or database administrators when to refresh their tables.

Standard Authority Identifier	**M**	The identifier of the federal, national or international organization that approved the data element domain value identifiers for a standard data element.
Justification Category	**M**	The classification of the positional alignment of domain values in a storage field.
Steward Name	**M**	Dependent on functional area (system generated based on the functional area identifier); a steward is responsible for certain functional areas and the validity of data contained in standard data elements within the functional area.
Derivation Code	**M**	Describes if the attribute and/or data element is atomic or the category of derivation. The two categories of derivation are derived and composite. **a. Composite data element**: Composite data elements describe multiple concepts. When a data element is formulated to describe multiple concepts, its definition and meaning can easily partially overlap with the definition of another data element. This redundancy sets the stage for data inconsistencies, increases system maintenance costs, and restricts the use of a data element to a narrow range of applications. When identifying a composite data element that is required to be used within a system, all pieces of data which make up this composite data element must be approved data elements within the DDDS. The names of the approved data elements that make up the composite should be recorded in the "comment text" field of the DDDS. **b. Derived data element**: Derived data elements represent the results of computational operations performed on other data elements. The computations may involve algorithms supported by two or more data elements within a single entity instance, or algorithms summarizing data element values across multiple entity instances within a single entity or across multiple entities. The algorithm is recorded in the "formula definition text" field of

		the DDDS.
Domain Value Type Identifier	**M**	Distinguishes the kinds of domain value identifiers in a data element (qualitative or quantitative) (system generated).
Authority Reference Text	**M**	The official regulation, policy, guidance, etc. that specifically requires the Department of Defense to capture, maintain, exchange this data; the text must directly reference the data. For any data element using the class word "IDENTIFIER" and proposed as a primary key attribute, this reference should describe the method for creating and maintaining the identifier, to ensure it's unique value across DoD.
Definition Text	**M**	The narrative describing the meaning of a standard data element.
Comment Text	**O**	Additional narrative description of a data element. This includes the method of creating and maintaining IDENTIFIERs when proposed as primary key attributes and the maintenance method is not addressed in the authority reference text.
Source List Text	**O**	The authoritative reference containing the official list of domain values.
Domain Definition Text	**M**	A narrative expressing the way the allowable domain value identifiers will be represented.
Domain Value Identifier	**C**	The actual codes that provide access to lists of categories of objects. A complete list of domain values is required for data elements having a specific domain.
Domain Value Definition Text	**C**	The narrative description and explanation of the domain value identifiers. Required if there are domain values.
Using Model Name	**M**	The association of a data element with one or more data models.
External Data Element Relationships	**C**	Provides a mapping to external data standards.

AP1.2.1. Data Element Quantitative Meta-data

ATTRIBUTE	OBLIGATION	ATTRIBUTE DEFINITION
Formula Definition Text	**C**	A narrative expressing the algorithm that calculates the value of a derived data element.
Unit Measure Name	**M**	The word and/or words that express the terms in which the dimension, quantity, or capacity of an object can be stated. a. "When Unit of Measure name is applicable and more than one possible unit of measure exists, two documentation options are available. If unit of measure is convertible to other units of measure through standard algorithms (i.e, Distance: feet converted to meters and vice versa), then the single most commonly used unit of measure should be entered. If multiple possible units of measure exist that cannot be converted using standard algorithms (i.e., Cable Quantity: cable by weight or cable by length), then a separate attribute (data element) should be added for managing and/or tracking the appropriate unit of measure for each instance of the entity." b. "N/A" is an acceptable entry for data elements classified as Date or Time.
Quantitative Accuracy Identifier	**M**	An indication of how accurate a data value must be.
Low Range	**C**	A string of up to 20 integers that indicates the smallest allowed domain value when a data element's domain is expressed as a range of acceptable values.
High Range	**C**	A string of up to 20 integers that indicates the largest allowed domain value when a data element's domain is expressed as a range of acceptable values.
Decimal Place Count Quantity	**C**	The integers that indicate the quantity of numeric digits allowed to the right of the decimal point in a quantitative fixed point domain value.

AP1.2.2. Data Element Qualitative Meta-data

ATTRIBUTE	OBLIGATION	ATTRIBUTE DEFINITION
Accuracy Number Percent	**M**	An indication of how accurate a qualitative domain value must be. Allowable values are 1-100 percent.

AP1.3. GENERIC ELEMENT META-DATA

ATTRIBUTE	OBLIGATION	ATTRIBUTE DEFINITION
Generic Element Name	**M**	The attribute that identifies the structure of a domain for data.
Counter Identifier	**M**	The "record number" within the DDDS (system generated); unique within a category of data standard.
Status Code	**M**	The stage within the approval cycle; system generated based on actions taken by the appropriate data administrators.
Service and/or Agency Component Code	**M**	The organization to which the creator is assigned.
Short Abbreviated Name	**M**	A short abbreviated name representing a specific generic element
Data Type Name	**M**	The name of the way domain values are stored in a database. The generic data elements with class words having a data type of "integer" will be modified with a comment (comment text field) as follows: Data element using the data type "integer" should fit into a 32 bit representation. The high range value of a signed integer is limited to "2.1 billion" (in the range -2^{31} to 2^{31}-1); data requirements of greater values should use the data types "floating point" or "fixed point".
Security Category	**M**	A classification assigned to the domain value identifiers stored in some physical media to show the level of protection required to prevent disclosure.
Maximum Character Count Quantity	**M**	The field length of the data; it should be large enough to accommodate all requirements, yet precise enough to allow for accuracy.

Standard Authority Identifier	**M**	The identifier of the federal, national or international organization that approved the data element domain value identifiers for a standard data element.
Justification Category	**M**	The classification of the positional alignment of domain values in a storage field (system generated).
Domain Value Type Identifier	**M**	Identifies domain values as quantitative or qualitative (system generated).
Authority Reference Text	**M**	The official regulation, policy, guidance, etc. that specifically requires the DoD to capture, maintain, exchange this data; the text must directly reference the data.
Definition Text	**M**	The narrative describing the meaning of a standard data element.
Comment Text	**O**	Additional narrative description of a data element. Any data elements using the class word "IDENTIFIER" and proposed as primary key attributes must indicate, in this field, the procedures for ensuring uniqueness of the key values or the name of the IS that creates and maintains the identifier.
Source List Text	**O**	The authoritative reference containing the official list of domain values.
Domain Definition Text	**M**	A narrative expressing the way the allowable domain value identifiers will be represented.
Domain Value Identifier	**C**	The actual codes that provide access to lists of categories of objects.
Domain Value Definition Text	**C**	The narrative description and explanation of the domain value identifiers. Required if there are domain values.

AP1.3.1. Generic Element Quantitative Meta-data

ATTRIBUTE	OBLIGATION	ATTRIBUTE DEFINITION
Low Range	**C**	A string of up to 20 integers that indicates the smallest allowed domain value when a data element's domain is expressed as a range of acceptable values.
High Range	**C**	A string of up to 20 integers that indicates the largest allowed domain value when a data element's domain is expressed as a range of acceptable values.
Decimal Place Count Quantity	**C**	The integers that indicate the quantity of numeric digits allowed to the right of the decimal point in a quantitative fixed point domain value.

AP2. APPENDIX 2

REVERSE ENGINEERING

AP2.1. INTRODUCTION

AP2.1.1. Reverse engineering the data requirements supported by an existing IS can be an effective way to establish useful data standards. In these cases, data requirements are inferred from existing operational data structures where the existing business process and supporting data have been determined to meet DoD data requirements. The difficulty with this approach is that existing data structures and processes are often poorly documented. Therefore, substantial effort is sometimes required to regenerate the baseline data requirements.

AP2.1.2. The purpose of reverse engineering is to extract data requirements from existing systems and their documentation. These data requirements can be used to create the data structures and standards supporting DoD activities and form a foundation for forward engineering.

AP2.1.3. Functional area integration managers often choose to document AS-IS data requirements for migration systems. Reverse engineering facilitates the evolutionary enhancements to migration systems. The scope of reverse engineering should be based on the following three factors:

AP2.1.3.1. Anticipated cost and benefits of the reverse engineering effort.

AP2.1.3.2. Degree of acceptable risk.

AP2.1.3.3. Degree of overlap between legacy and migration systems.

AP2.1.4. Figure AP2-F1 illustrates some of the complexity in assessing cost and/or benefits and risk connected to initiating reverse engineering efforts. Reverse engineering may be useful in describing the data requirements supported by the information systems and identifying overlap among systems.

AP2.2. PRODUCTS OF REVERSE ENGINEERING

AP2.2.1. Figure AP2-F2 illustrates the role of reverse engineering in the reengineering process. The reengineering process consists of reverse engineering and forward engineering:

AP2.2.1.1. Reverse engineering captures descriptive information about the current system and consists of recovery of AS-IS physical objects and documenting the existing AS-IS design.

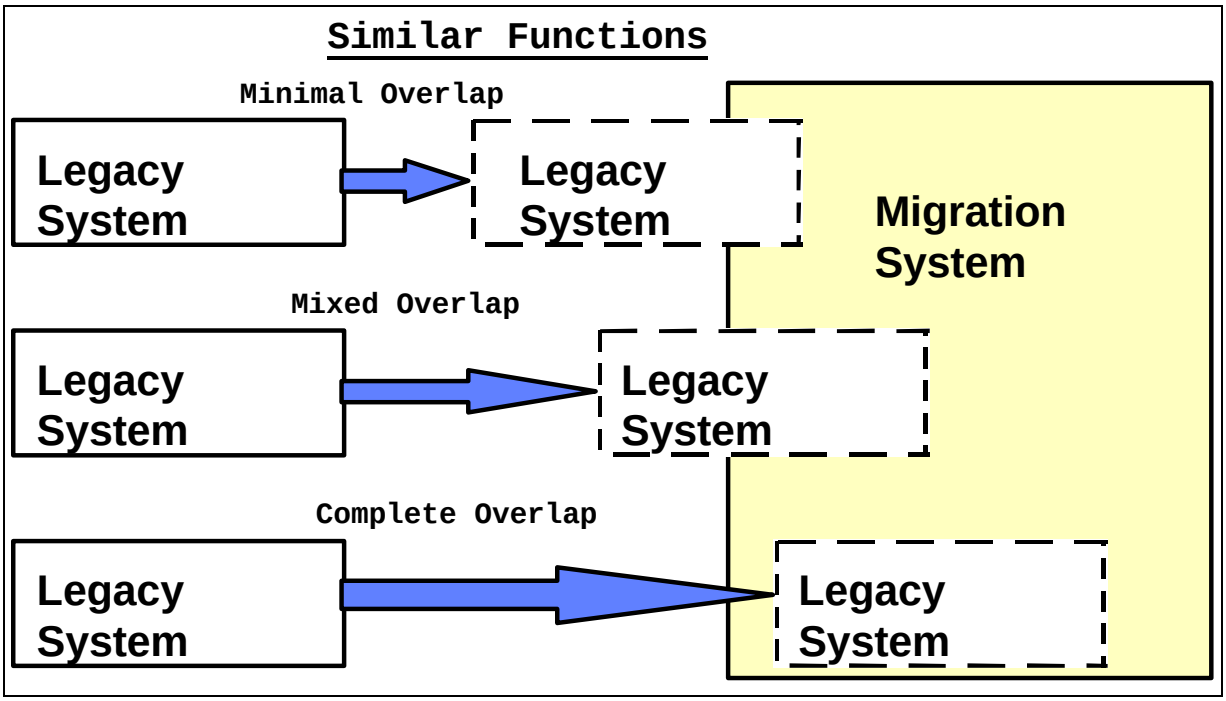


Figure AP2-F1 Reverse Engineering Data Requirements

AP2.2.1.2. Forward engineering designs and develops the TO-BE system and consists of describing the future TO-BE design and generation and maintenance of the TO-BE system.

AP2.2.2. Reverse engineering products should be stored in a repository or library for future reference and use. The repository or library need not be a sophisticated electronic device but must facilitate reference and use in the subsequent processes of reengineering. The goal of reverse engineering is to produce two products: recovery of physical objects and documentation of the existing design:

AP2.2.2.1. Recovery of Physical Objects

These products are primarily the collection of information that describes the physical system. In poorly documented systems, the recovery of physical characteristics includes capture of:

AP2.2.2.1.1. Data sets created, managed, and used by the system (e.g., tables, input transactions, reports, query screens, interface documentation).

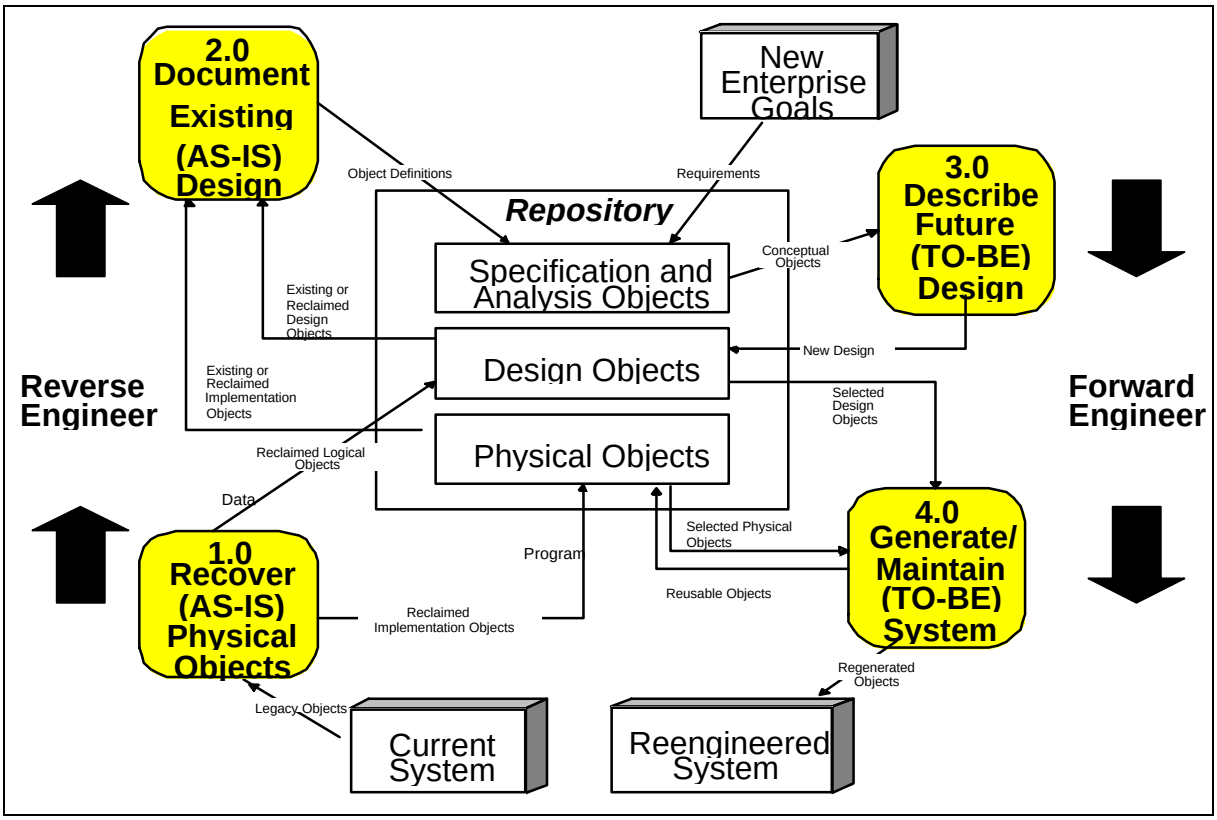


Figure AP2-F2 The Reengineering Process

AP2.2.2.1.2. Information about the data. For example, the name of the data field, definition of the data, type of data (e.g., alphabetic or numeric), domain values.

AP2.2.2.1.3. Source code, libraries, and schemas maintained by organization(s) having configuration management responsibilities for the system.

AP2.2.2.1.4. Policies, directives, instructions, and/or regulations that authorize the use, creation, operation, and/or maintenance of the system.

AP2.2.2.1.5. System specifications that were used to build the system (e.g., System Requirements Specification (SRS), System Design Document (SDD), Database Specification, Functional Description (FD)).

AP2.2.2.1.6. Object recovery involves the collection and cataloguing of all documentation describing the IS. Establishing the reverse engineering library is a significant task and will require the cooperation of functional area experts, system administrators, and operations and maintenance personnel.

AP2.2.2.2. Documentation of Existing Design

AP2.2.2.2.1. These products focus on recapturing the current design of an IS. Using the catalogue of information that has been collected through the recovery of physical objects that describe an IS, the current design is documented as a set of models that describes the essential requirements being satisfied by the current system.

AP2.2.2.2.2. Several types of models and diagrams can be used. Decomposition diagrams, dependency diagrams, data flow diagrams, and IDEF0 diagrams describe the flow of data within a system. Data structure diagrams, entity-relationship diagrams, and IDEF1X data models (in third normal form (3NF) and fully attributed) document the meaning and interrelation of data.

AP2.3. THE REVERSE ENGINEERING PROCESS

Figure AP2-F3 illustrates the four phases of reverse engineering projects that successfully link reverse engineered data models to the DoD data standardization initiative. The processes are generally sequential and may be iterative. The first column describes the roles and responsibilities needed to perform reverse engineering.

AP2.3.1. Data Collection

AP2.3.1.1. The first phase of reverse engineering is to identify the migration and legacy systems that are to be reverse engineered and catalogue the physical information that describes the IS. Generally, functional areas working reverse engineering efforts recognize that not every system is a candidate for reverse engineering. For example, migration systems that are well documented and can be modified easily to support added requirements are not good candidates for reverse engineering. Migration systems that are not well documented and cannot be easily modified may be good candidates for reverse engineering.

AP2.3.1.2. Basically there are three circumstances for reverse engineering an IS:

AP2.3.1.2.1. The system is a migration system that is not well documented. Nevertheless, the system will be enhanced or modified to incorporate additional requirements.

AP2.3.1.2.2. The system is a legacy system that is not well documented and will be incorporated, replaced, or interfaced to designated migration systems. Under this scenario, the legacy system data requirements are documented and these requirements are compared to those satisfied by an existing migration system.

Comparing requirements satisfied by each system, is an aid in data conversion, data quality improvement, and/or migration system enhancement efforts.

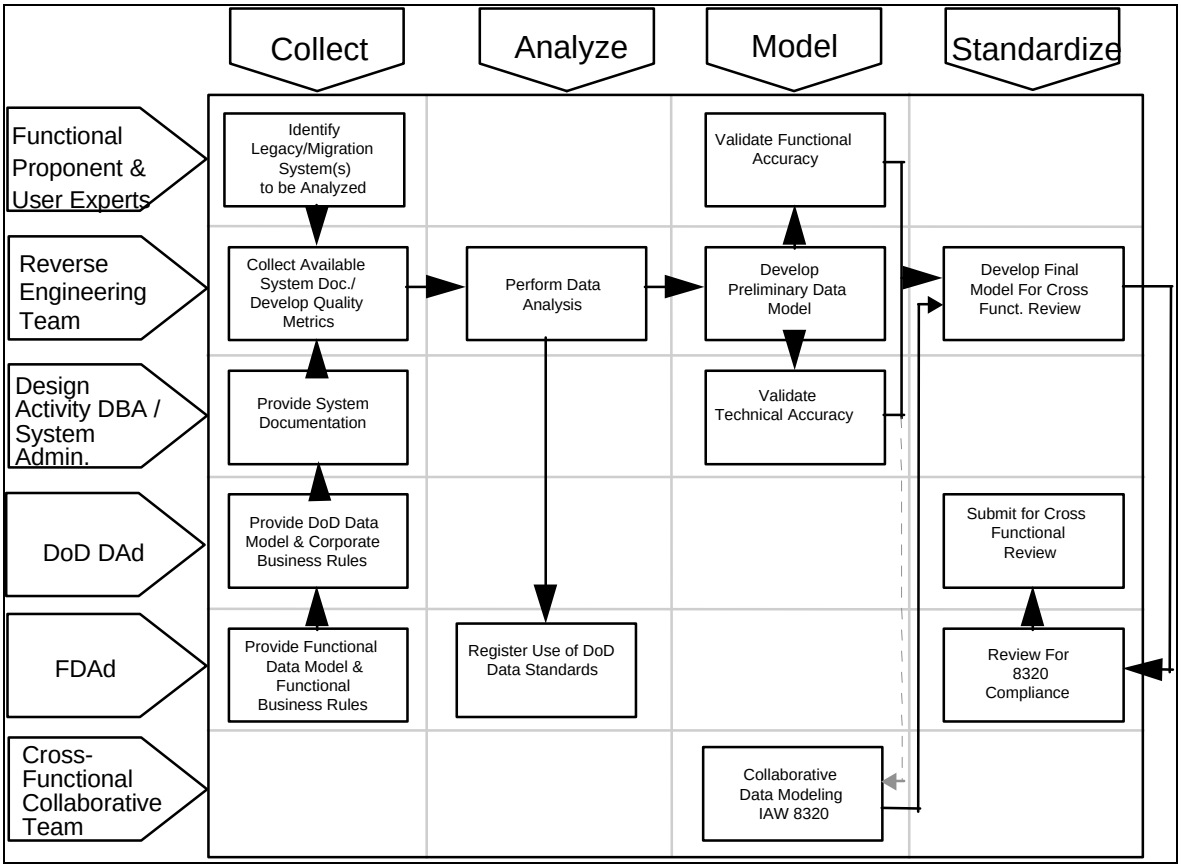


Figure AP2-F3 Reverse Engineering and Relationship to DoD Standardization

AP2.3.1.2.3. The system is either a legacy or migration system which is well documented and contains data which are currently shared across multiple applications.

AP2.3.1.3. As part of cataloguing the physical information that describes the IS, there are many sources of system documentation. The system administrators, database administrators, and organizations responsible for the design and configuration management of the system are excellent sources of information. DoD functional proponents and end users should be able to provide useful information on the system.

AP2.3.1.4. There are several considerations that may affect the success of the reverse engineering effort:

AP2.3.1.4.1. Quality of Documentation

The amount, accuracy, and currency of documentation on an existing IS varies significantly. The reverse engineering team must be resourceful in finding documentation that represents the current system.

AP2.3.1.4.2. Use of the DDM and DDDS

It is advisable to make use of the DDM and the DDDS to the maximum extent possible in performing data analysis and data modeling tasks. These sources of information represent the authoritative source of DoD data standards and should be put to use in all data analysis and data modeling efforts. Access should be obtained to the DDDS through the DoD DAd.

AP2.3.2. Data Analysis

AP2.3.2.1. The reverse engineering team performs data analysis and data modeling. This is followed by validation in collaborative sessions with functional experts and technicians. Catalogued data is examined and a set of data requirements is produced for the system. This baseline should be specified in terms of the current dictates of the system environment within a particular organization.

AP2.3.2.2. Data specifications may be divided into four critical areas for documentation:

AP2.3.2.2.1. Data element specification consisting of DoD data element meta-data.

AP2.3.2.2.2. Data structure specification consisting of use of data model entity, attribute and description.

AP2.3.2.2.3. Business rules consisting of data constraints, updates, creation, and availability.

AP2.3.2.2.4. Further detail descriptions of how much, who, where, and when data is to be used.

AP2.3.2.3. Data analysis requires the complete description of data requirements and an examination of common and unique data characteristics. Three types of descriptive information are captured in connection with reverse engineering:

AP2.3.2.3.1. Data Set Information

Data needs supported by a legacy or migration system are found on transactions, data interchange requirements, message

formats, forms, master files, records, or tables. One of the first steps in understanding data is to describe the types of data sets that are used by the legacy or migration system. General information on data sets include:

AP2.3.2.3.1.1. Data set name and brief description of information content and purpose of data set.

AP2.3.2.3.1.2. Identification of regulation or instruction controlling the creation, management, or use of the data set.

AP2.3.2.3.1.3. Identification of Component or Service that makes use of the data set.

AP2.3.2.3.1.4. Name of IS that supports the creation, management, or use of the data set.

AP2.3.2.3.1.5. Additional information collected on data sets (e.g., tables, records, master files) include: size, volume, and frequency of update. Data analysts often focus their attention on priority data sets.

AP2.3.2.3.1.6. Priority data sets are typically identified as critical functional needs that warrant a complete and unequivocal description. For example, reverse engineering efforts in the DoD Finance and Procurement areas may focus reverse engineering on the unmatched disbursement problem and the subsystems, modules, files, and interchange requirements supporting contract payment, accounting, and disbursement.

AP2.3.2.3.2. Data Element Information

AP2.3.2.3.2.1. Much of the detailed work in reverse engineering is to collect information about the data that resides on each data set (e.g., table, master file, interchange requirement). The DoD data analysts should collect the meta-data described in AP1. Appendix 1.

AP2.3.2.3.2.2. This meta-data information should be captured on data items that reside on data sets. This detailed information may only be collected on data sets representing priority functions of the physical or internal data structures supported by an IS. In addition, information on concatenated, grouped, coupled, and multi-purpose data items used in an IS may be useful.

AP2.3.2.3.3. Comparative Information

AP2.3.2.3.3.1. This data analysis task establishes whether data requirements supported by a designated migration or legacy system are already described as a DoD data standard, or valid developmental data standards for DoD data standardization. The comparative analysis results are documented in a traceablity matrix. This establishes a mapping between the DoD standard and the data element within the system. For example, National Item Identification Number (NIIN) is a data element found in many DoD systems. It is used to uniquely identify catalogued supply items in the DoD inventory. This data element has the same characteristics as the DoD data standard: Materiel-Item-Supply Identifier.

AP2.3.2.3.3.2. The reconciliation and integration of the data requirements are used to develop the pool of data elements and/or data standards that are matched and mapped to existing DoD data standards, or proposed data standards. Detailed procedures for matching and mapping data standards are provided in AP3. Appendix 3.

AP2.3.3. Data Modeling

In situations where existing application data elements cannot be matched or mapped to DoD data standards, the reverse engineering team should use modeling techniques to describe data requirements. In performing this analysis, two types of models are beneficial:

AP2.3.3.1. Decomposition Diagrams

In reverse engineering DoD systems, it is often wise to breakout large complex systems into simpler units or modules. Simpler units of the systems are reverse engineered to focus attention on relevant aspects of the problem. As shown in Figure AP2-F4, the decomposition diagram is used to decompose a complex activity into simpler units.

AP2.3.3.2. Data Models

AP2.3.3.2.1. IDEF1X data modeling (FIPS PUB 184, reference (b)) has been established as the DoD standard for data model representation. Data modeling during reverse engineering creates a blueprint of the data requirements in terms of entities, attributes, and relationships. Typically, this AS-IS model can be developed quite rapidly from the data sets (e.g., tables, master files, and record layouts) that are supported by the existing IS.

AP2.3.3.2.2. Figure AP2-F5 provides the data model that was developed from the source on country codes. The first table contains information on countries and includes: Country Code, Country Name, and Scope Note. The second table contains information on principal subdivisions for countries and includes: Country Code plus a number to uniquely identify the subdivision of the country, Subdivision Name (e.g., Alabama), and Subdivision type name (e.g., province, territory, state).

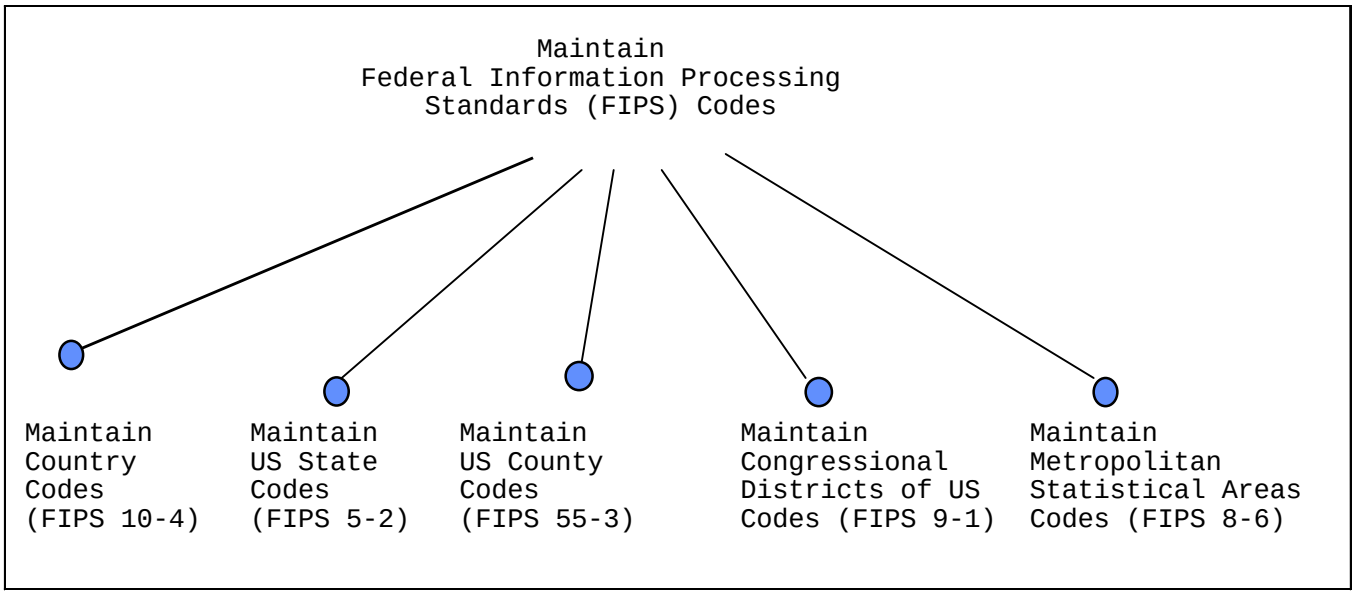


Figure AP2-F4 Decomposition Diagram

AP2.3.3.2.3. In reverse engineering, as shown in Figure AP2-5, the physical tables become entities (e.g., COUNTRY and COUNTRY-PRINCIPAL-DIVISION) and the columns of the physical tables become attributes in the data model (e.g., COUNTRY Code, COUNTRY Name, COUNTRY-PRINCIPAL-DIVISION Name).

AP2.3.3.2.4. The amount of data modeling is dependent on the scope and the objectives of the project. Reverse engineering focuses on retaining the features of data as they exist in a system while using current data modeling techniques. Reverse engineering builds a data model that results in the following:

AP2.3.3.2.4.1. The logical model should be a higher level of abstraction than a physical schema.

AP2.3.3.2.4.2. The entities and attributes are named by functional experts.

AP2.3.3.2.4.3. The degree of normalization is limited to the original physical normalization of the data reflected in the system.

AP2.3.3.2.4.4. The data model preserves the original scope of the reverse engineering effort.

AP2.3.3.2.4.5. The data requirements exclude any additional requirements or desired requirements identified during reverse engineering.

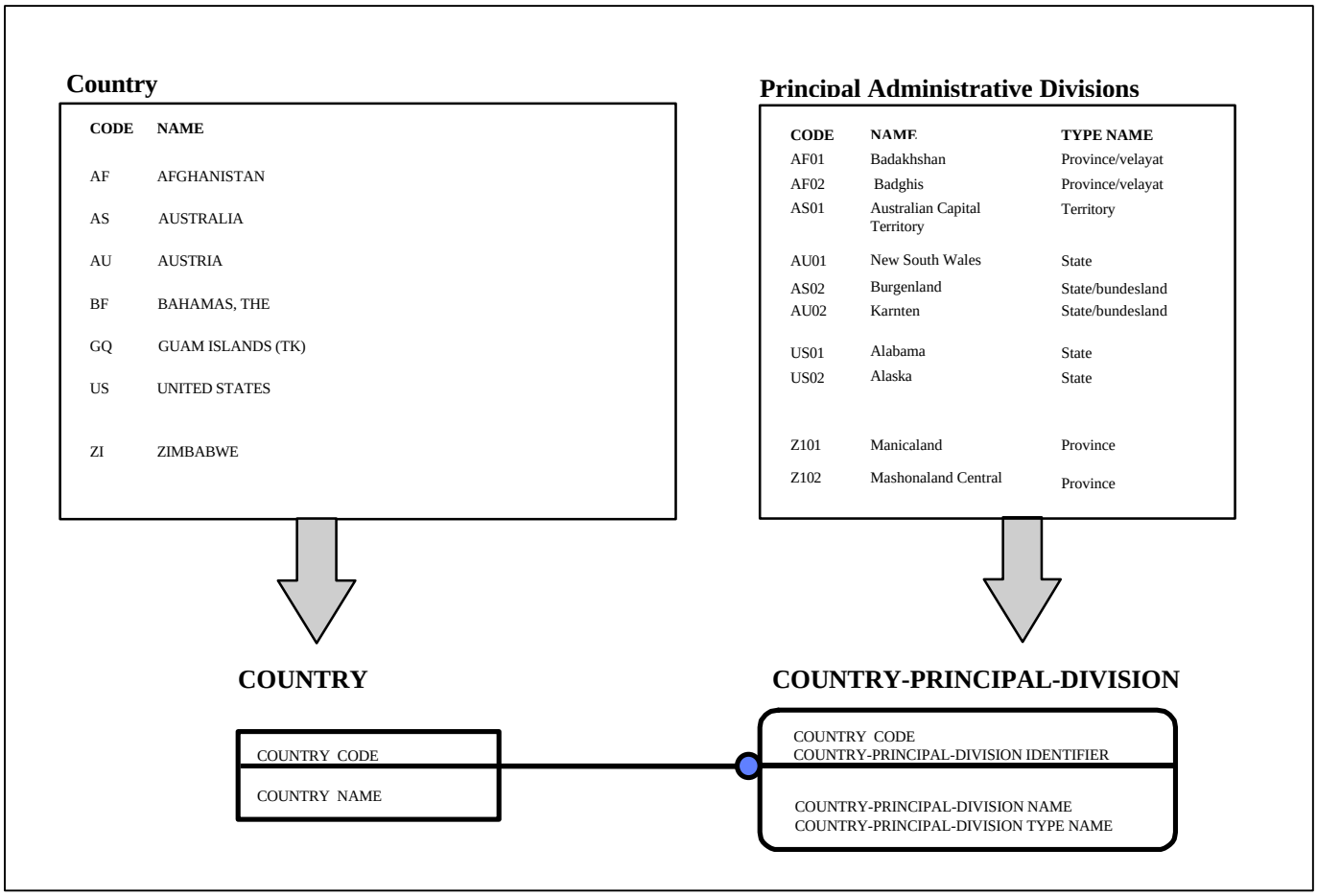


Figure AP2-F5 FIPS 10-4 Physical Tables and Data Model

AP2.3.3.2.4.6. The syntax of data modeling is applied without changing (such as correcting) the data requirements as supported by the system.

AP2.3.3.2.5. Although data models document some conditions and constraints, further details must be provided to ensure adequate restrictions have been inferred and are specified. Business rules are the constraints that define the creation, update and deletion of values that data elements can undergo and remain consistent.

AP2.3.3.2.6. Reverse engineering must document how data is organized and structured. Several kinds of structures need to be documented:

AP2.3.3.2.6.1. User Views. The data elements that are presented to users as outputs (reports, screens, etc.) need to be listed and their interrelationships documented.

AP2.3.3.2.6.2. Input Views. Data elements collected from user screens should be described.

AP2.3.3.2.6.3. Storage Views. Files and data base records should be carefully documented.

AP2.3.3.2.6.4. Transaction Views. Sets of data elements that create, update or delete storage structures must be described.

AP2.3.3.2.7. For large, complex systems, these views should be merged and integrated into a "data model" which summarizes the data structure requirements for the system as a whole.

AP2.3.4. Data Standardization

Documented data requirements derived from the reverse engineered data models should then be brought forward for standardization by the reverse engineering team. These data requirements shall be standardized in accordance with the procedures established in this document.

AP2.4. ALTERNATE REVERSE ENGINEERING PROCESS

Alternatively, the Reverse Engineering for Data Integration and Sharing (REDIS) methodology may be utilized. The intent of reverse engineering utilizing the REDIS methodology is to normalize the legacy system logical model to Third Normal Form (3NF). This then allows comparision of the legacy system to the DoD data dictionary and mapping/matching of the legacy system entities and data elements for data standardization.

AP3. APPENDIX 3

BASELINING THE USE OF DoD DATA STANDARDS: MATCHING AND MAPPING TO STANDARDS

AP3.1. INTRODUCTION

This guidance is focused on the data engineering analyses that are required to baseline the use of DoD standard data elements in DoD information systems (IS). As an initial step in implementing data standards, recording the relationship between application data and existing data standards is critical. First, matching and mapping application data to standard data elements establishes a baseline of standard data elements that are used by an IS. Second, the creation of the baseline allows IS designers and developers to measure progress towards implementing standard data elements. Third, the implementation of data standards is closely tied to improving data sharing, data interchange, and our ability to get the correct information to the Warfighter at the right time. Importantly, improving data sharing, system integration, data quality and utility are critical Command, Control, Communications, Computers and Intelligence (C4I) interoperability goals. These C4I For The Warrior (C4IFTW) goals have driven the establishment of over 15,000 data standards that are stored in the Defense Data Dictionary System (DDDS). These goals are the central theme of the DoD data standardization initiative that emphasizes the importance of improving the Warfighter's information as a key ingredient in maintaining mission readiness, improving reliability and enhancing effectiveness through technological superiority.

AP3.2. WHEN TO MATCH OR MAP TO DoD DATA STANDARDS

Matching and mapping application data to DoD data standards establishes what data elements in an existing IS are similar or dissimilar to the data standards that have been approved by the Department.

AP3.2.1. IS Lifecycle Considerations

The decision to match and map for planning and design purposes is guided by IS lifecycle considerations. As shown in Figure AP3-F1, matching and mapping for planning purposes is performed either early in the system lifecyle or in situations where systems are implemented or deployed. This type of matching and mapping is performed to support the future use of data standards. The second type of matching and mapping is typically more appropriate in situations where analysis and design tasks are being performed. Matching and mapping is not a substitute for using standard data in systems development and modernization.

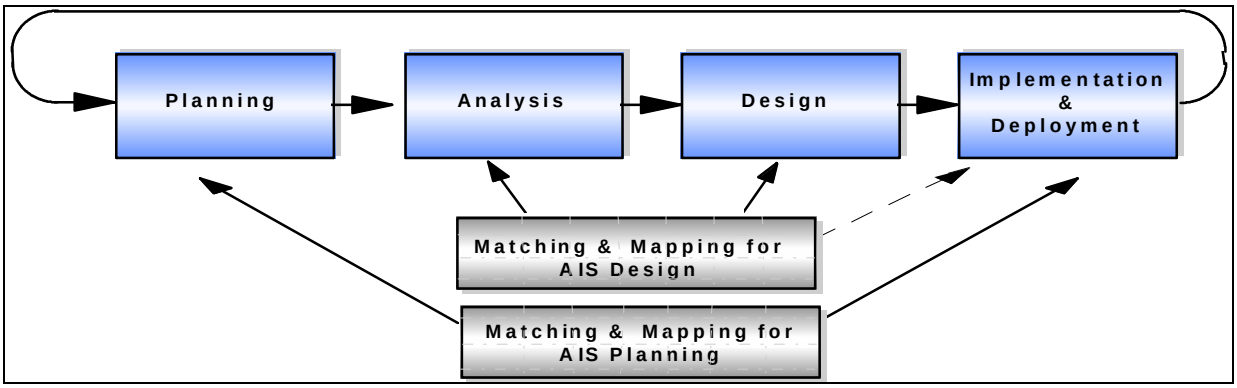


Figure AP3-F1: Using Data Standards: Matching and Mapping Occurs Throughout the IS Lifecycle.

AP3.2.2. Performing Matching and Mapping Analysis

Data Administrators will compare existing data within ISs against DoD data standards to:

AP3.2.2.1. Support the adoption of standard data elements in parallel with modernizing, enhancing, modifying, and improving systems.

AP3.2.2.2. Support the migration of data from existing data stores and databases to databases using DoD standard data.

AP3.2.2.3. Facilitate the capture of performance metrics established by the Department.

AP3.2.3. Using the DDDS to Match and Map

The DDDS recognizes two types of matching and mapping. First, in support of migration planning, the DDDS facilitates the recording of matches and mappings for planning purposes. This type of matching and mapping records whether an application data element matches or can be mapped to an established standard. The second type of matching and mapping is for IS managers who are designing IS capabilities or moving data from legacy systems to databases that use DoD data standards. The DDDS supports recording of business rules that define the relationship between legacy application data elements and DoD data standards.

AP3.3. MATCHING AND MAPPING CRITERIA

AP3.3.1. Figure AP3-F2 provides the criteria used to match or map application data to DoD data standards. It is the responsibility of the Functional Data Administrator (FDAd) and

functional area experts to support matching and mapping of application data elements to DoD data standards.

Attributes	Matching	Mapping	Matching and Mapping Notes
Name	Not Mandatory	Not Mandatory	Functional name for data element.
Class Word	Equivalent, if the application data carries a class word	Equivalent, if the application data carries a class word	Not mandatory in situations where application data elements do not carry a class word designation. If a class word does exist, the class words for application data elements are to be equivalent to the class word of the approved DoD data standard (e.g., NAME as a class word is equivalent to TEXT; The class word CODE, however, is not equivalent to NAME or TEXT.
Access Name	Not Mandatory	Not Mandatory	It is not likely that the access name for an existing application data element will be identical to the access name stored in the DDDS. In addition, requiring an equivalent access name is not meaningful. For these reasons, the access name does not have to be identical or equivalent. It should be noted, however, that developers should use the DDDS access name in implementing standard data elements, wherever practical.
Definition Text	Equivalent	Equivalent	Word for word definitions may be rare. For atomic data, definition should be similar. For derived or composite data, definitions are different, but should, in part, be related to the standard.
Data Value Source List Text	Not Mandatory	Not Mandatory	Use of the same reference text is a good indicator that the application data element is the same as the DoD data standard. However, several references may contain identical information.
Data Type Name	Equivalent	Not Mandatory	Matching and/or Mapping Note: See discussion on DDDS and SQL data types.
Maximum Character Count Quantity	Equivalent	Not Mandatory	Matching and/or Mapping Note: See discussion on DDDS data types, signed data, DATE as data type and field lengths.
Decimal Place Count Quantity	Identical	Not Mandatory	Used on quantitative data elements to record scale.
Domain Value Identifiers	Identical	Equivalent	For an application data element with specific domain values, all domain value identifiers must be identical to the standard to have a match. This includes the Domain Value Identifier Text. Data elements with subsets of the standard domain values are a subset match.
Domain Value Identifier Text	Identical	Equivalent	The domain value text for the application data element must also be identical to have a match. Voids and subsets to the standard domain value text are subset match.
High-Range Identifier	Equivalent	Not Mandatory	See discussion on signed data, DATE as data type, and field lengths.
Low-Range Identifier	Equivalent	Not Mandatory	See discussion on signed data, DATE as data type, and field lengths.
Unit of Measure Name	Identical	Equivalent	Applies to quantitative data elements. (E.G.., Pounds, Liters)
Security Classification Name	Identical	Identical	Security classification must be the same.
Formula Definition Text	Equivalent	Not Mandatory	For matching purposes, formula for deriving a application data element from other application data should be equivalent to formula used to derive a data standard from other data standards.

Figure AP3-F2: Matching and Mapping Criteria

AP3.3.2. Personnel performing matching and mapping use a variety of sources for completing the registration of application data to standards. Characteristics listed in Figure AP3-F2 are found in the following sources: database specification, data dictionary, database schema, domain or reference tables and file descriptions supporting the application. Database schemas and file sections contain information such as Access Name (column name), Data Type Name, and Maximum Character Count Quantity.

AP3.3.3. In matching application data to DoD standards, there are several criteria that deserve attention:

AP3.3.3.1. Definition must be equivalent.

AP3.3.3.2. Data Type must be equivalent. See Figure C7-F2 for DDDS data types and DBMS equivalents.

AP3.3.3.3. Maximum Character Count Quantity (Field Length) must be equivalent.

AP3.3.3.4. For fixed decimal place data elements, digits to the right and left of the decimal point must be the same.

AP3.3.3.5. For data elements using the class word CODE, the application data element must make use of all the allowable Domain Value Identifiers AND the associated Domain Value Description Text. Subset mappings are identified when an application data item implements a subset of the valid Domain Value Identifiers and Domain Value Descriptions.

AP3.3.3.6. For quantitative data elements, the low range and high range values for the application data element must be equivalent to the respective low range and high range values prescribed for the data standard.

AP3.3.3.7. For quantitative data elements, units of measure must be the same (e.g., pounds, feet, meters).

AP3.3.3.8. The DDDS may record the low range for a standard data element by placing a negative sign in the Low Range Identifier. The low range may be -999.99 with Maximum Character Count Quantity of 7 to account for the negative sign and decimal point. Many commercial off the shelf (COTS) database management systems (DBMS) handle both signed data and placement of a decimal point by using precision and scale variables. The application data element matches the standard where the appropriate precision and scale is equivalent. Under SQL compliant databases the following is equivalent to the DDDS specification for -999.99: NUMERIC (5,2). Additional high and low range values and data Specifications supporting these values are shown in Figure AP3-F3.

High and Low Range	SQL Data Types	Sybase Data Specification	Oracle Data Specification
+999999.99 - 999999.99	NUMERIC, DECIMAL	NUMERIC(8,2)	NUMBER(8,2)
+99.9999 -99.9999	NUMERIC,DECIMAL	NUMERIC(6,4)	NUMBER(6,4)
+9999.99999 - 9999.99999	NUMERIC,DECIMAL	DECIMAL(9.5)	NUMBER(9,5)
+99.9 -99.9	NUMERIC,DECIMAL	DECIMAL(3,1)	NUMBER(3,1)

Figure AP3-F3: DDDS High Range and Low Range Values and Physical Data Specifications

AP3.4. MATCHING DATA ELEMENTS

For an application data element to match a DoD data standard, all data characteristics that describe potential data values must be identical. Figure AP3-F4 illustrates a data element from the Global Command and Control System (GCCS) AIRFIELDS application that matches the DoD data standard for country code.

Attributes	DoD Data Standard	AIRFIELDS
Name	COUNTRY CODE	COUNTRY CODE
Class Word	CODE	CODE
Access Name:	CY-CD	CY_CD
Definition Text:	THE CODE THAT REPRESENTS A COUNTRY.	THE CODE THAT REPRESENTS A COUNTRY.
Data Value Source List Text:	FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION 10-4,...	AAFIF Product Specification
Data Type Name:	CHARACTER-STRING	CHAR
Maximum Character Count Quantity	2	2
Decimal Place Count Quantity	NA	NA
Domain Value Identifiers & Domain Value Identifier Text	ID TEXT AF AFGHANISTAN AG ALGERIA AL ALBANIA AN ANDORRA AO ANGOLA AQ AMERICAN SAMOA AR ARGENTINA AS AUSTRALIA AU AUSTRIA : :	ID TEXT AF AFGHANISTAN AG ALGERIA AL ALBANIA AN ANDORRA AO ANGOLA AQ AMERICAN SAMOA AR ARGENTINA AS AUSTRALIA AU AUSTRIA : :
High Range Identifier	NA	NA
Low Range Identifier	NA	NA
Unit of Measure Name	NA	NA
Security Classification Name	UNCLASSIFIED	UNCLASSIFIED
Formula Definition Text:	NA	NA

Figure AP3-F4: Matching an Application Data Element

AP3.5. MAPPING TO DATA STANDARDS

Four types of mappings are possible: subset, atomic, concatenated and derived. In mapping application data elements to DoD data standards for design purposes, all variances between the data characteristics of the application data element and the standard data element will be recorded. For example, differences may include a formula or algorithm used to derive the application data element from two or more DoD data standards.

AP3.5.1. Subset Matches: Mapping Designation

Application data elements that are a subset of the domain values in the DoD data standard will be documented as a subset match. For example, applications using only the country codes for North Atlantic Treaty Organization (NATO) nations, may use a subset of the country codes shown in Figure AP3-F5. When an

Attributes	DoD DATA STANDARD	NATO COUNTRY CODE
Name	COUNTRY CODE	NATO_COUNTRY CODE
Class Word	CODE	CODE
Access Name:	CY-CD	NATO_CTRY_CD
Definition Text:	THE CODE THAT REPRESENTS A COUNTRY.	THE CODE THAT DENOTES A COUNTRY WITH MEMBERSHIP IN THE NORTH ATLANTIC TREATY ORGANIZATION.
Data Value Source List Text:	FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION 10-4,...	--
Data Type Name:	CHARACTER-STRING	CHAR
Maximum Character Count Quantity	2	2
Decimal Place Count Quantity	NA	NA
Domain Value Identifiers & Domain Value Identifier Text	ID TEXT BE BELGIUM : : CA CANADA : : DA DENMARK : : FR FRANCE : :	ID TEXT BE BELGIUM : : CA CANADA : : DA DENMARK : : FR FRANCE : :
High Range Identifier	NA	NA
Low Range Identifier	NA	NA
Unit of Measure Name	NA	NA
Security Classification Name	UNCLASSIFIED	UNCLASSIFIED
Formula Definition Text:	NA	NA

Figure AP3-F5: Subset Match to Existing DoD Data Standard

application data element is identified as a subset match to an existing data standard the application data element is entered to the DDDS as a non-standard data element. After entry, the DDDS functions for establishing a relationship between a non-standard (i.e., application data item) and a standard data element should be used.

AP3.5.2. Atomic Data Element Mapping

AP3.5.2.1. Atomic data elements are data elements that represent a single concept. Figure AP3-F6 provides information on three atomic data elements for the identification of countries. Although, the data element names are similar, other data characteristics are not the same. Critical differences are shown in Domain Value Identifiers and Domain Value Definition Text.

AP3.5.2.2. For example, although the application data element, COUNTRY CODE, from the Air Force Flying Training Programming and Accounting System (FTPAS) uses many of the same domain values as under the DoD data standard (e.g., AR = ARGENTINA), the application data element is missing the value for AMERICAN SAMOA and has a different Domain Value Identifier for AUSTRALIA (i.e. AT). The variance from the standard should be entered in the DDDS.

Attributes	DoD Data Standard	External Standard Data Element	Application Data Element
Name	COUNTRY CODE	COUNTRY CODE	COUNTRY CODE
Class Word	CODE	CODE	CODE
Access Name	CY-CD	CTRY-CD	COUNTRY
Definition Text	THE CODE THAT REPRESENTS A COUNTRY.	THE CODE THAT DENOTES A COUNTRY.	
Data Value Source List Text	FIPS 10-4	ISO 3166	AIR EDUCATION AND TRAINING COMMAND (AETC) PAMPHLET 51-6
Data Type Name	CHARACTER-STRING	CHARACTER-STRING	CHARACTER-STRING
Maximum Character Count Quantity	2	2	2
Decimal Place Count Quantity	--	--	--
Domain Value Identifiers & Domain Value Identifier Text	ID TEXT AF AFGHANISTAN AG ALGERIA AL ALBANIA AN ANDORRA AO ANGOLA AQ AMERICAN SAMOA AR ARGENTINA AS AUSTRALIA AU AUSTRIA : :	ID TEXT AF AFGHANISTAN DZ ALGERIA AL ALBANIA AD ANDORRA AO ANGOLA AS AMERICAN SAMOA AR ARGENTINA AU AUSTRALIA AT AUSTRIA : :	ID TEXT AF AFGHANISTAN AG ALGERIA AL ALBANIA AN ANDORRA AO ANGOLA AR ARGENTINA AT AUSTRALIA AU AUSTRIA : :
High Range Identifier	--	--	--
Low Range Identifier	--	--	--
Unit of Measure	--	--	--
Security Classification	Unclassified	Unclassified	Unclassified
Formula Definition	--	--	--

Figure AP3-F6: Atomic Mapping

AP3.5.3. Concatenated Data Element Mapping

AP3.5.3.1. Sometimes, application data elements are concatenated or grouped. A concatenated data element is a data element that is not single concept. Figure AP3-F7 illustrates the mapping between contract number and established data standards.

Figure AP3-F7: Concatenated Data

AP3.5.3.2. Contract number as the application data element should be loaded in the non-standard partition of the DDDS and mapped to each of the standards represented by the four data items. The business rule(s) that describe the grouping should be entered in the DDDS. For example, for design purposes the following information should prove useful in adopting the DoD data standard for contract number. The application data element appears in **BOLD** text and the DoD standards appear in *italics*.

CONTRACT NUMBER consists of the following DoD standard data elements:

1 - 6 *ORGANIZATION-DESIGNATOR IDENTIFIER*
7 - 8 *PERIOD IDENTIFIER* (FISCAL YEAR)
9 *CONTRACTING-AGREEMENT INSTRUMENT TYPE CODE*
10 - 13 *CONTRACTING-AGREEMENT SEQUENCE IDENTIFIER*

AP3.5.4. Derived Data Element Mapping

AP3.5.4.1. Application data elements can be calculated or derived from DoD data standards. These application data elements are entered into the DDDS as non-standard data and are mapped to DoD standards. Figure AP3-F8 illustrates three application data elements from GCCS AIRFIELDS that map to multiple DoD data standards.

DoD Data Standard	Application Data Element
AIRPORT-APRON-TYPE WIDTH DIMENSION AIRPORT-APRON-TYPE LENGTH DIMENSION	APRON TOTAL SQUARE AREA
AIRPORT-DINING-FACILITY NORMAL PERSONNEL COUNT QUANTITY AIRPORT-DINING-FACILITY PERSONNEL TYPE CODE	OFFICERS MESSING NORMAL QUANTITY
AIRPORT EQUIPMENT TYPE COUNT QUANTITY AIRPORT-EQUIPMENT CATEGORY CODE	CRASH EQUIPMENT CODE

Figure AP3-F8 Derived Data Elements Mapped to DoD Data Standards

AP3.5.4.2. In mapping derived data elements for IS system design purposes, the business rules that describe the derivation or calculation between application data elements and standards should be entered in the DDDS. Derivations can be entered using pseudo-code, SQL statements, algebraic or numeric formulas, or a clear set of English statements.

AP4. APPENDIX 4

PROCEDURES FOR REUSING EXISTING DATA STANDARDS

AP4.1. INTRODUCTION

AP4.1.1. The DoD data dictionary is the authoritative source for DoD data standards. The dictionary contains approved standard data with related meta-data and provides documentation of the life cycle events for standard data. The data dictionary also functions as the managerial tool for storing developmental, candidate, and non-standard data, as well as applicable external data standards.

AP4.1.2. The DDM provides the overall logical view of the DoD data requirements. The DDM stores and depicts the business rules that specify how entities relate to one another. Reviewing the entities and their relationships facilitates sharing of existing data standards and reduces the requirement to develop new proposed data standards.

AP4.1.3. This appendix also addresses the adoption of external data standards as DoD standards. External data standards are those standards that are maintained outside the DoD, and are used within DoD ISs.

AP4.2. REUSE EXISTING DATA ELEMENT STANDARDS

Review the current generic elements, external standards, and DoD standards in the DoD data dictionary and the DDM for reuse. All data requirements should fall into one of these categories:

AP4.2.1. Data standard meta-data exactly matches data requirement. If an existing data element is an exact match for the proposed data requirement, use the existing standard. Register your application’s use of attributes in the DoD data dictionary. Relate the existing standard to the IS and using model information. This information becomes an important part in performing impact analysis of changes and archival of existing standards. Procedures for registering the use of data standards are delineated in AP3. Appendix 3.

AP4.2.2. Data standard with overlapping or subset data domains of data requirement. If the data requirement’s data domain is overlapping with an existing standard, it is possible the existing standard may need to have its domain extended. This can be recommended as a modification to an existing standard.

AP4.2.3. Data standard is equivalent with different domain value representations. In the situation where a data requirement

is the same as an existing data element, but the domain values are captured in dissimilar representations (for example values “1 to 5” versus the data standard values “a to e”), map to the existing element and describe the mapping of the domain values to the existing data element domain values for the purpose of transition to the DoD data standard. Alternately, the data requirement can be modified to reflect the domain value representation of the DoD data standard. Procedures for matching and mapping data standards are delineated in AP3. Appendix 3.

AP4.2.4. Data standard is similar, but uses a different format than the data requirement. If an existing data standard represents the same information concept as a data requirement but uses a different format (e.g. 8 character numeric, vs 4 character alpha), a different domain set (not a 1 to 1 mapping), or in other ways is very different than the data requirement, a decision must be made: Whether to adopt the data standard and abandon the unique requirement; or to modify the existing data standard to mirror the data requirement. Modifications to data standards must be supported by documentation (regulations, etc…) that show how the modification is more correct than the existing data standard. Modifications without such documentation will carry little weight, and may not be accepted. Developers should be biased in favor of adopting data standards and abandoning unique data requirements whenever possible.

AP4.2.5. No existing standard for data requirement. When no existing element represents the same data requirement, then create a new data standard as described in C5. Chapter 5.

AP4.3. MODEL AND ENTITY REUSE

Examine existing entities in the DoD data dictionary and the DDM for reuse. The following guidelines are provided for this process:

AP4.3.1. Finding an entity with the same business rules and attributes as the data requirements. If an existing entity in the DDM represents the data requirement (including the same business rules and attributes), use the existing entity and attributes.

AP4.3.2. Finding an entity with a subset of attributes. In reviewing the DDM, if an existing entity contains a subset of the required attributes use the existing entity. Represent the missing data requirements by developing new attributes for the existing entity.

AP4.3.3. Finding a standard entity with a subset of required business rules. If entity relationships (business rules) in the

DDM represent some of the required business rules, determine if the existing business rules are sufficient. Accommodate new requirements by adding new business rules to the entity, or by modifying existing meta-data for entities or attributes.

AP4.3.4. When existing business rules and entities do not address the requirements, propose new entities, attributes and business rules to the DDM. Defining a new independent entity is encouraged, when required. This is preferred to compromising a business rule to support artificial relationships.

AP4.3.5. Matching issues. Two issues frequently appear in attempting to compare data requirements to existing data standards. The issues are:

AP4.3.5.1. Synonyms. Synonyms are two or more occurrences of the same data item with differing names. An in depth review of existing standards meta-data must be performed. The resolution of synonyms requires involvement by both functional and technical experts and provides one of the greatest benefits to a data administration program by reducing the number of data items to manage, increasing the accuracy and integrity of databases, and increasing interoperability between systems.

AP4.3.5.2. Homonyms. Homonyms are two different data items which share the same name. Superficial use of analytical techniques for homonym location may cause false matching of data requirements.

AP4.4. ADOPTING EXTERNAL DATA STANDARDS FOR DoD USE

DoD policy requires that the DoD adopt applicable federal, national, and international data standards before creating DoD data standards. These data standards should be reused to the maximum extent practicable. External data standards are those standards which have been adopted by federal, national and international standards bodies such as the American National Standards Institute (ANSI), Federal Information Processing Standards (FIPS), International Organization for Standardization (ISO), North Atlantic Treaty Organization (NATO). Two types of external data standards may be adopted: reference data and data interchange standards:

AP4.4.1. Reference Data.

AP4.4.1.1. Reference data standards are established by federal, national, and international standards organizations to capture a list of valid values for data elements. As reference data, the standardization of valid values supports a uniform representation of data in reference files or domain tables.

Examples of reference data include: Country Codes (FIPS 10-4 & ISO 3166), Office of Personnel Management Codes (FIPS 95-1), and U.S. State Codes (FIPS 5-2) (reference (k)). The adoption of external reference data as DoD data standards follows the same procedures used to standardize any other data requirement within the DoD, with emphasis placed on the following:

AP4.4.1.1.1. The requirement for the use of the external standard must be established and the DDDS must be checked to determine whether the data requirement has already been adopted as a DoD data standard.

AP4.4.1.1.2. If the standard has not been adopted, a proposal package, integrating this data requirement within the DDM, must be prepared.

AP4.4.1.1.3. The functional data steward having responsibility for the applicable functional area shall assign its Functional Area Identifier to the external data standard.

AP4.4.1.1.4. The Authority Reference Text shall specify the external data standard reference and title.

AP4.4.1.1.5. The standard must be coordinated with other DoD functional areas.

AP4.4.1.2. The coordination activity validates the use of the external standard and the completeness of the descriptive information about the standard (e.g., data type name, maximum character count quantity, domain value identifiers, domain value identifier text).

AP4.4.1.3. Other issues that may be addressed by the cross functional review are stewardship, naming conventions, and placement of the external data in the DDM.

AP4.4.2. Data Interchange Standards.

AP4.4.2.1. Data interchange standards are used in batch oriented data exchange. These standards are represented by both the DoD messaging standards, such as United States Message Text Format (USMTF) and Variable Message Format (VMF), and standards promoted under Electronic Commerce and/or Electronic Data Interchange (EC/EDI). Data interchange standards and implementation conventions are established, validated, and approved by the DoD messaging and EC/EDI communities.

AP4.4.2.2. The messaging standards are based on functionally validated data interchange needs with the trend toward the development of joint messaging standards that can be used by the

DoD Commander-In-Chiefs (CINCs), Military Services, and Defense Agencies.

AP4.4.2.3. The EC/EDI standards that are used in the DoD are based on work by the ANSI ASC X12 committee. The ANSI ASC X12 transaction sets have been adopted as the standard for the exchange of data between the Government and industry. As a federal partner in using the X12 transaction sets, the DoD participates in federal functional working groups to develop X12 implementation conventions. These conventions document how the X12 transaction sets are to be used by the Department of Defense.

AP4.4.2.4. The adoption of external interchange data as DoD data standards requires somewhat different procedures than those used to standardize other data requirements within the DoD:

AP4.4.2.4.1. DoD data administrators (FDAds and CDAds) are encouraged to work with the functional communities involved in messaging and EC/EDI standards. In working with interchange standards, data administrators should be aware that data interchange standards coexist with other data standards.

AP4.4.2.4.2. Some of the external reference data that are used on ANSI ASC X12 transaction sets include: Codes for Representation of Names of Countries (ISO 3166); Codes for Representation of Currencies and Funds (ISO 4217); Standard Color and Size Codes (National Retail Merchants Association); Financial Information Reporting Codes (Treasury Management Association); Current Procedural Terminology (CPT) Codes (American Medical Association); National Drug Code (Food and Drug Administration); and Standard Industrial Classification Codes (National Technical Information Service).

AP4.4.2.4.3. The requirement for the use of the data interchange standard must be established and the DDDS must be checked to determine whether the data requirement has already been adopted as a DoD data interchange standard. Messaging standards will be assigned an appropriate ASD(C3I) Functional Area Identifier by the data steward. ANSI X12 data interchange standards have been assigned Functional Area Identifier 082.

AP4.4.2.4.4. If the standard has not been adopted, a proposal package must be prepared. However, these data requirements will not be integrated with the DDM.

AP4.4.2.4.5. Interchange data will be loaded within a separate set of tables within the DDDS under the appropriate Functional Area Identifier.

AP4.4.2.4.6. The Authority Reference Text shall specify the external data standard reference and title.

AP4.4.2.4.7. The standard must be coordinated with other DoD functional areas.

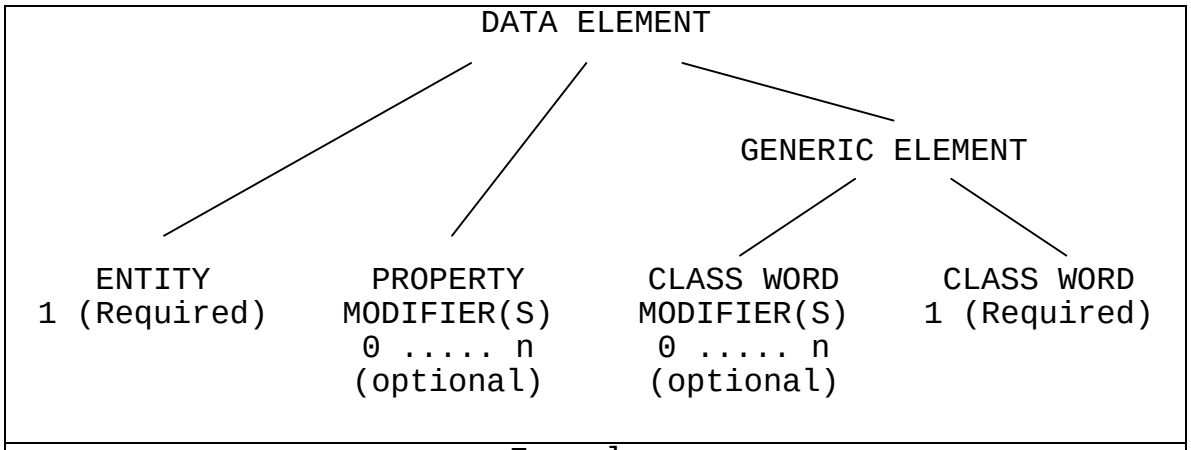
AP4.4.2.5. The coexistence of data standards has important implications for the DoD data administration community. First, data interchange standards are functionally approved standards that promote data shareability. For example, the ANSI ASC X12 standards have been specifically designed to provide a uniform representation of data so that trading partners share the same data definitions. Second, data interchange standards may be somewhat unique in that the definition of data is highly dependent on context.

AP5. APPENDIX 5

DATA STANDARDS NAMING AND DEFINITION GUIDELINES

AP5.1. DATA ELEMENT NAME COMPONENTS

A data element, as represented in the DoD data dictionary, is an entity attribute identified in a logical data model. At a minimum, a data element name consists of an entity and a generic element. Generic elements approved for use are documented and maintained in the DoD data dictionary. Generic elements are used to classify data elements based upon domains, representation, storage or usage. Optional modifiers may be used to clarify the content of the data element. The data element name format is as depicted in Figure AP5-F1:



Examples:

CUSTOMER			NAME
CUSTOMER		MONTH	CODE
CUSTOMER	DELIVERY	MONTH	CODE
CUSTOMER	DELIVERY		CODE

Figure AP5-F1 Data Element Name Format

AP5.1.1. Entity Name (Mandatory)

An entity represents a set of real or abstract things (people, objects, places, events, combination of things, etc.) identified in a logical data model. Data element names are based on an entity represented in the logical data model. Words used as entities in some data element names may be used as modifiers in other data element names.

AP5.1.2. Property Modifier (Optional)

A property modifier is a word that is used to further refine or describe an entity or a generic element, but does not dictate the structure (maximum size or data type; e.g., real, integer, character) of the data element.

AP5.1.3. Class Word Modifier (Optional)

A class word modifier is a word (adjective) that is used to further refine or describe a class word. The use of modifiers is optional and should be minimized. When used, a class word modifier must distinguish one generic element from another and narrow the range of the allowable domain values for the class word. The class word modifier along with a class word make up a generic element name.

AP5.1.4. Class Word (Mandatory)

AP5.1.4.1. A class word is a noun that designates the general category of data at the highest level and subcategorizes data elements based on like meta-data. Class words, with or without modifiers, are known as generic elements. Modifiers used with class words create new generic elements. This combination further defines the class word; e.g., Latitude Coordinate. The class word DATE can not be implemented as a generic element. To be a valid generic element, it must be used with an approved modifier, such as: Calendar Date, Ordinal Date, Year Date, etc.

AP5.1.4.2. All data elements are required to fit into a class. The list of available class words is depicted in Figure AP5-F2. Refer to the DoD data dictionary for the class word meta-data descriptions. There are two types of class words: qualitative and quantitative. Qualitative class words provide a means to identify the instance of a data element. Quantitative class words not only provide the means to identify, but also measure the instance of a data element. Qualitative class words are not intended for mathematical computations. Quantitative class words may be used for mathematical computations. If a new data element cannot fit into a class, then a proposal may be submitted to the DoD DAd to create a new class word (generic element).

AP5.1.4.3. The domain (permissible set of values) for a data element is established by the generic element and may be either specific or general in nature. A specific domain has a finite definition and an enumerable set of data values. A general domain has a broad definition and a large (possibly infinite) set of acceptable values that cannot be enumerated within reason.

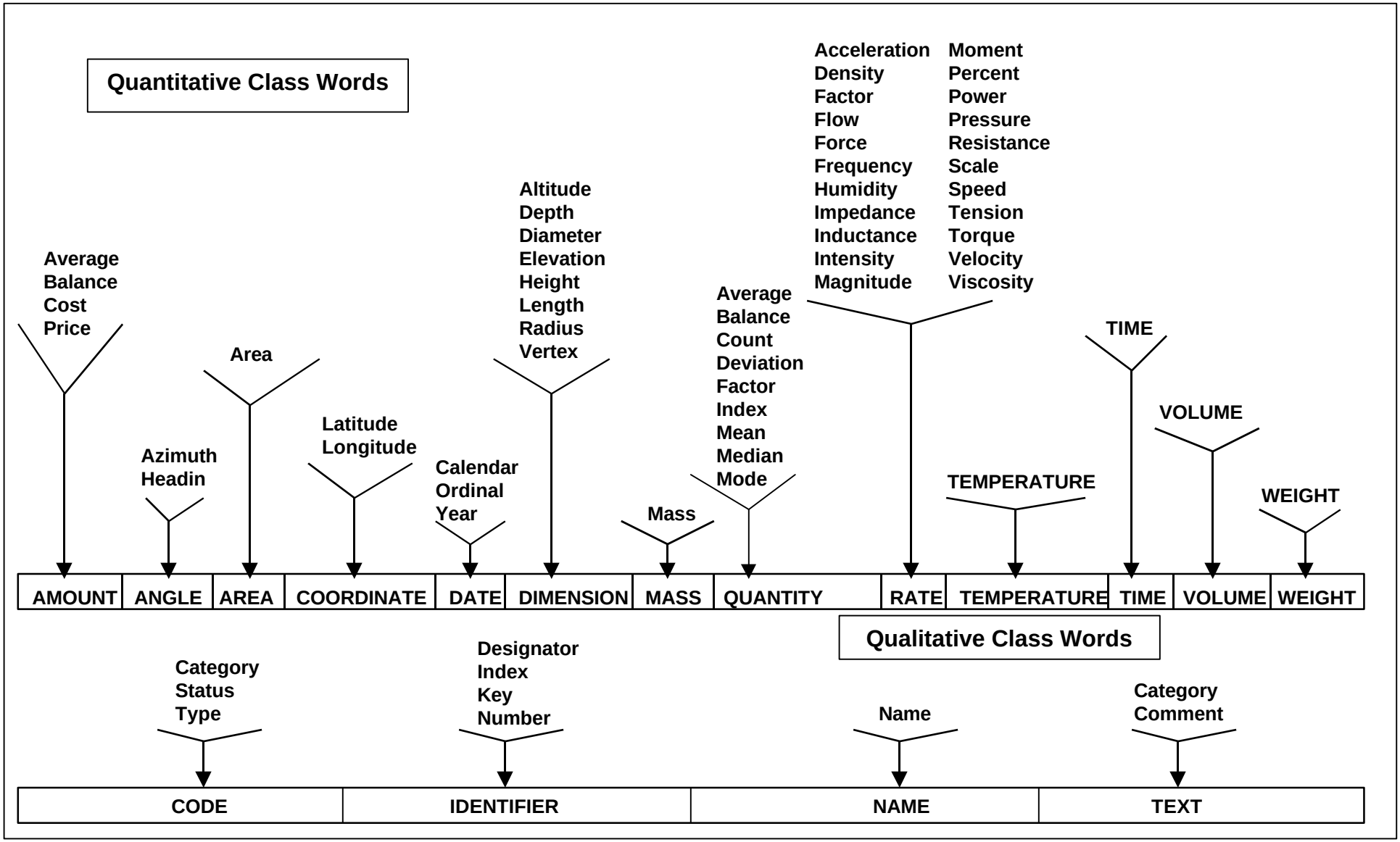


Figure AP5-F2 Guide for Selecting DoD Class Words

AP5.2 ENTITY NAMING GUIDELINES

AP5.2.1. The entity name shall:

AP5.2.1.1. Be a singular noun or noun phrase.

AP5.2.1.2. Include only alphabetic characters (A-Z) and hyphens (-) (i.e., MEDICAL-FACILITY, MATERIEL-ITEM). Hyphens are used when the name consists of multiple words.

AP5.2.2. The entity name should NOT contain:

AP5.2.2.1. Class word names except under special circumstances. Approved class word names may be used in entity names (such as PERSON-NAME) to more clearly identify an information requirement commonly used in the business. An entity name should not be just a class word name.

AP5.2.2.2. Abbreviations or acronyms unless they have been approved and are contained in the DoD data dictionary.

AP5.2.2.3. Names of organizations, computer or information systems, directives, forms, screens, or reports.

AP5.2.2.4. Articles (a, an, the) or prepositions (at, by, for, from, in, of, to, etc.) unless the article or preposition clearly aids in identifying an information requirement term commonly used in the business.

AP5.3. ENTITY DEFINITION GUIDELINES

The entity definition should:

AP5.3.1. Define WHAT the entity is, not HOW, WHERE, or WHEN the entity is used, or WHO uses it.

AP5.3.2. Add meaning to the name. Do not merely restate or rephrase the name, or just provide a list of the attributes or meta-attributes within the entity.

AP5.3.3. Be concise. The definition should be brief and comprehensive.

AP5.3.4. Be precise and unambiguous. The exact meaning and interpretation of the defined concept should be apparent from the definition. A definition should be clear enough to allow only one possible interpretation.

AP5.3.5. Avoid circular reasoning. Two definitions should not be defined in terms of each other. Avoid one definition pointing

to a second definition for further explanation and the second definition pointing back to the first definition.

AP5.3.6. NOT contain examples. A definition should be able to stand alone. Examples may be captured as separate comments in the comment text field in the DoD data dictionary.

AP5.3.7. NOT contain infinitives to begin the definition (e.g., "This entity defines..." or "To describe...").

AP5.4. GENERIC ELEMENT NAMING GUIDELINES

The generic element name shall consist of either:

AP5.4.1. A class word only.

AP5.4.2. A class word and modifier(s).

AP5.5. GENERIC ELEMENT DEFINITION GUIDELINES

Class word definitions are listed in Figure AP5-F3.

CLASS WORD NAME	ABBREVIATION	DEFINITION
Amount	AM	A monetary value. The data element definition should begin: "The (modifiers) amount of"
Angle	AN	The rotational measurement between two lines and/or planes diverging from a common point and/or line. The data element definition should begin: "The (modifiers) angle between (modifiers) for a"
Area	AR	The two dimensional measurement of a surface expressed in unit squares. The data element definition should begin: "The (modifiers) area of"
Code	CD	A combination of one or more numbers, letters, or special characters substituted for a specific meaning. The data element definition should begin: "The (modifiers) code that represents and/or denotes a"
Coordinate	CN	One of a set of values which identifies the location of a point. The data element definition should be: "The coordinate identifying the (modifiers) location of"

Date	DT	The notation of a specific period of time. The data element definition should begin: "The (modifiers) date of and/or when and/or on which a"
Dimension	DM	A one dimensional measured linear distance. The data element definition should be: "The dimension (length, width, height, radius, or elevation, etc.) of and/or from"
Identifier	ID	A combination of one or more numbers, letters, or special characters which designates a specific object and/or entity, but has no readily definable meaning. The data element definition should begin: "The (modifiers) identifier that represents"
Mass	MS	The measure of inertia of a body. The data element definition should begin: "The (modifiers) mass of"
Name	NM	A designation of an object and/or entity expressed in a word or phrase. The data element definition should begin: "The name of"
Quantity	QY	A nonmonetary numeric value. The data element definition should begin: "The (modifiers) quantity of"
Rate	RT	A quantitative expression that represents the numeric relationship between two measurable units. The data element definition should begin: "The rate of"
Temperature	TP	The measure of heat in an object. The data element definition should begin: "The temperature of"
Text	TX	An unformatted character string generally in the form of words. The data element definition should begin: "The text of"
Time	TM	A notation of a specified chronological point within a period. The data element definition should begin: "The time of"
Volume	VL	A measurement of space occupied by a three dimensional figure. The data element definition should begin: "The volume of"

Weight	WT	The force with which an object is attracted toward the earth and/or other celestial body by gravitation. The data element definition should begin: "The weight of"

Figure AP5-F3 Class Word Definitions

AP5.6. DATA ELEMENT NAMING GUIDELINES

5.6.1. The data element name shall:

AP5.6.1.1. Be based on the entity name it is associated with.

AP5.6.1.2. Be a singular noun phrase.

AP5.6.1.3. Include only alphabetic characters (A-Z), hyphens (-), and spaces ( ).

AP5.6.1.4. Separate each component of the name by a space.

AP5.6.2. The data element name should NOT contain:

AP5.6.2.1. Abbreviations or acronyms unless they have been approved and are contained in the DoD data dictionary.

AP5.6.2.2. Names of organizations, computer or information systems, directives, forms, screens, or reports.

AP5.6.2.3. Articles (a, an, the) or prepositions (at, by, for, from, in, of, to, etc.) unless the article or preposition clearly aids in identifying an information requirement term commonly used in the business.

AP5.6.2.4. The possessive forms of a word, i.e., a word which denotes ownership.

AP5.7. DATA ELEMENT DEFINITION GUIDELINES

The data element definition should:

AP5.7.1. Define WHAT the data is, not HOW, WHERE, or WHEN data are used or WHO uses the data.

AP5.7.2. Be comprised of a grammatically and structurally correct, simple sentence(s).

AP5.7.3. Represent a characteristic of its associated entity. It is acceptable to use the actual entity and generic element name in the definition. If the entity and generic element name

are used in the definition there is no need to redefine these terms.

AP5.7.4. Spell out any acronyms and abbreviations.

AP5.7.5. Be concise. The definition should be brief and comprehensive.

AP5.7.6. Be precise and unambiguous. The exact meaning and interpretation of the defined concept should be apparent from the definition. A definition should be clear enough to allow only one possible interpretation.

AP5.7.7. Avoid circular reasoning. Two definitions should not be defined in terms of each other. Avoid one definition pointing to a second definition for further explanation and the second definition pointing back to the first definition.

AP5.7.8. NOT contain examples or physical characteristics of the data element. A definition should be able to stand alone. Examples may be captured as separate comments in the comment text field in the DoD data dictionary.

AP5.7.9. NOT contain infinitives to begin the definition (e.g., "This data element defines..." or "To describe...").

AP5.8. EXCEPTIONS

AP5.8.1. Exceptions to these guidelines will be considered on a case-by-case basis. If unique business requirements dictate changes to these guidelines (common business terminology, existing external data standards, etc.), the appropriate Component or Functional Data Administrator will document the required exceptions and request they be considered for approval during the cross functional review process.

AP5.8.2. Exceptions will be granted by the DoD Data Administrator if no significant objections from the data administration community are raised during the cross functional review process.

AP6. APPENDIX 6

DoD DATA MODELING GUIDANCE

AP6.1. INTRODUCTION

IDEF1X has been established as the DoD standard technique for data model presentation and integration. DoD rules, syntax, and techniques for IDEF1X are presented in reference (b). This appendix addresses DoD-specific data modeling guidelines not explicitly covered in reference (b).

AP6.2. RELATIONSHIP VERB PHRASES

AP6.2.1. Relationship verb phrases represent business rules (statements or facts that define the constraints and relationships between entities). Each business rule statement should be constructed so that the parent entity name is the subject, the relationship name is the verb phrase, and the child entity name is the object.

AP6.2.2. All data models submitted should have relationship labels. The relationships should be named with active tense verb phrases. Verbs of being (has) and auxiliary verbs (is, was) should be avoided. The emphasis is on providing meaningful information about the organization’s business through the model.

AP6.3. CATEGORY (SUBTYPE) ENTITIES

AP6.3.1. A category, or subtype, entity captures a subset of the instances of a parent entity (referred to as a generalization entity, or generic parent). A “category cluster” is a set of one or more categorization relationships. The goal of category entities is to form non-overlapping subsets of instances of the parent entity distinguished by a category discriminator. Each category entity inherits common attributes and relationships from the parent, including its primary keys (which become foreign keys in the category entity). The category entity contains additional attributes and relationships that are related to the parent, but that are distinct from other related subsets. It contains some attributes and relationship(s) that apply only to instances of the subset and not to all instances of the parent.

AP6.3.2. In a “complete” categorization, every instance of the parent entity is associated with an instance of a category entity. In an “incomplete” categorization, an instance of the parent entity can exist without being associated with an instance

of any of the category entities. When a category cluster is identified as “complete”, the cluster must contain at least two subtypes of the parent entity.

AP6.3.3. When a parent entity is categorized, a discriminator is used to associate the category entities with their related parent entity. A discriminator is a non-key attribute that links the category entities with the parent by providing a meaning for the subtyping relationship. Therefore, it is imperative that the discriminator be named. Discriminators need to be labeled when a categorization is complete or incomplete. No two category clusters of a parent entity may have the same discriminator. The discriminator attribute must have a specific domain, containing domain values that discriminate one category of the parent entity from the others.

AP6.3.4. Subtypes of the same parent entity cannot have any other relationship between them; subtypes can only be related through the supertype. A relationship between subtypes of the same parent entity indicates a recursive relationship of the parent entity.

AP6.4. ROLE NAMING

A role name is defined as a name for the function that the foreign key attribute plays in the entity. When there are multiple migrations of a key to an entity, role names should be used to prevent the unification of the migrating keys. The role names distinguish the different roles the key plays. This is the only case in which role names should be used. Role names do not become DoD data standards; only the original name of the attribute is standardized (as a data element). Role names should be indicated on the logical data model. If a hierarchy exists, the appropriate business word(s) that best describe the requirement for that attribute should be used. If the role names are not provided, the terms “ORDINATE” and “SUBORDINATE” may be used. Figure AP6-F1 illustrates the method for labeling role names on the logical data model.

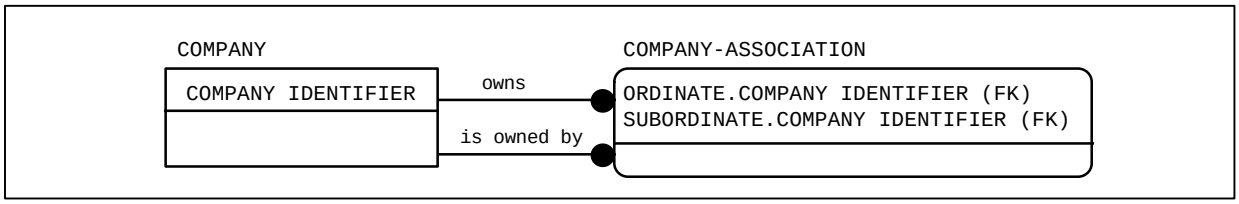


Figure AP6-F1 Entity Labeling Rule for Role Names

AP6.5. ASSOCIATIVE ENTITIES

AP6.5.1. Recursive Associations

AP6.5.1.1. In a recursive association, an entity is both the parent and the child; the entity is related to itself.

AP6.5.1.2. Recursive relationships can be represented in two formats: hierarchical, which is a relationship to itself; and network, which uses dual relationships to portray recursive entity associations. These formats are shown in Figure AP6-F2.

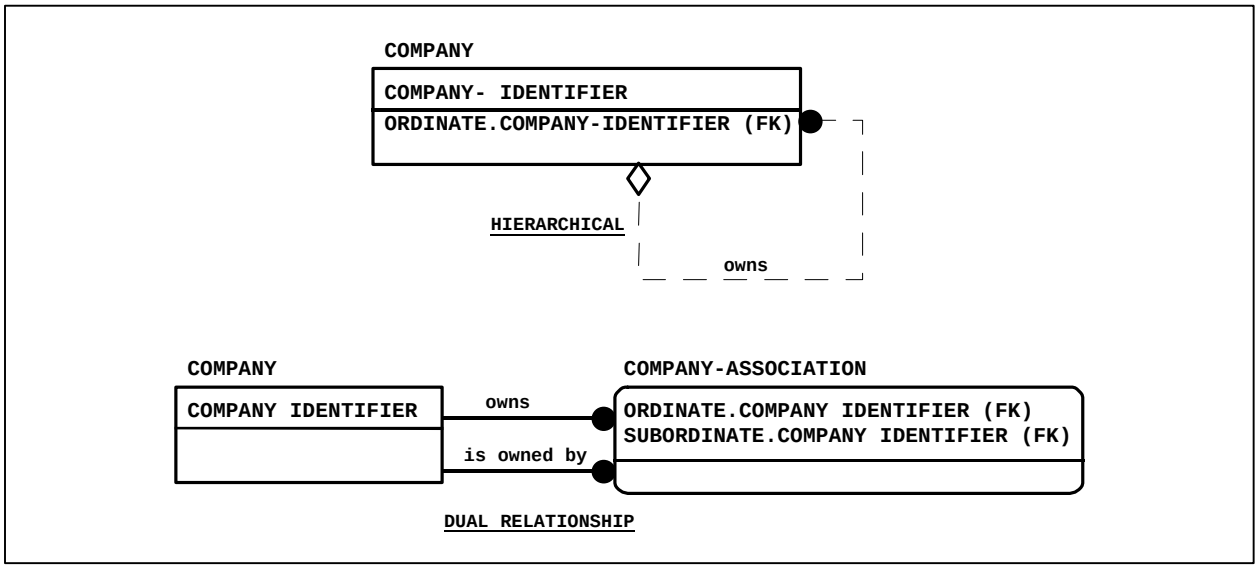


Figure AP6-F2 Hierarchical vs. Dual Relationship Recursions

AP6.5.1.3. In naming the entity used to represent the recursive association, the format illustrated in Figure AP6-F2 shall be applied; that is, the term “ASSOCIATION” should be appended to the name of the parent entity to form the name of the associative entity (COMPANY-ASSOCIATION).

AP6.5.1.4. In defining the entity used to represent the recursive association, the format shall be as follows: “An association of a COMPANY with another COMPANY.”

AP6.5.2. Resolution of Many-to-Many (non-specific) Relationships

AP6.5.2.1. A non-specific relationship, referred to as a “many-to-many relationship,” is an association between two entities in which each instance of the first entity is associated with zero, one, or many instances of the second entity and each

instance of the second entity is associated with zero, one, or many instances of the first entity.

AP6.5.2.2. Many-to-many relationships must be resolved for a logical data model in 3NF. This is accomplished through an associative entity, as illustrated in Figure AP6-F3.

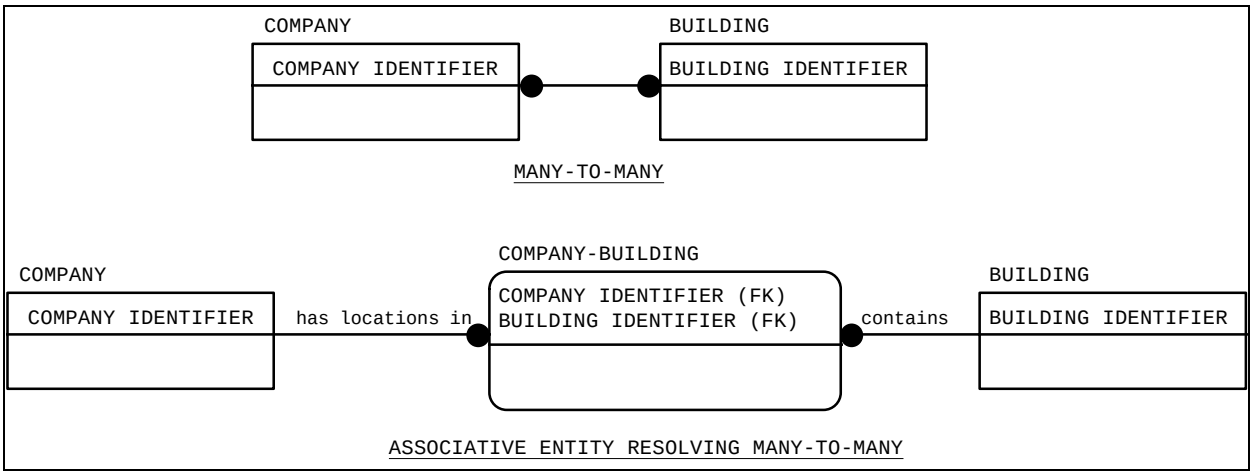


Figure AP6-F3 Resolution of a Many-to-Many Relationship

AP6.5.2.3. In naming the associative entity used to resolve a many-to-many relationship, the suggested format illustrated in Figure AP6-3 shall be applied; that is, the names of the two parent entities should be combined to create the name for the associative entity (COMPANY-BUILDING).

AP6.5.2.4. In defining the associative entity used to resolve a many-to-many relationship, the suggested format shall be used as in the following example: “An association of a COMPANY with a BUILDING.”

AP6.5.3. Associations with Native Attributes

AP6.5.3.1. The intersection of two entities may represent a true object for the function. In this case, the associative entity may have native key or non-key attributes. This type of association is illustrated in Figure AP6-F4:

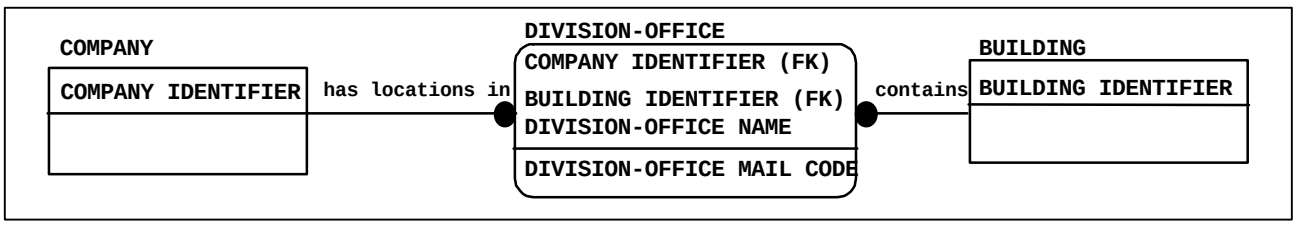


Figure AP6-F4 Associative Entity with Native Attributes

AP6.5.3.2. In naming the associative entity which represents a true object for the function, the actual name of the object may be used.

AP6.5.3.3. The associative entity should be defined in a manner which clearly describes the information captured within the entity.

AP6.6. ERD PRESENTATION GUIDELINES

AP6.6.1. All ERDs distributed as part of a cross functional review package will conform to the following presentation guidelines:

AP6.6.1.1. All entities and attributes (both proposed and those annotated “For Display Purposes Only”) will comply with the following font style standard:

Approved - **Bold** (Arial 10)
Candidate - *Italicized* (Arial 10)
Developmental - Normal font (Arial 9)
For Display Purposes Only - * (All entities and attributes shown for “For Display Purposes Only” will be designated with an asterisk (*), to be placed at the beginning of the name.)

AP6.6.1.2. All entities and attributes will be written in uppercase letters, as in the DDM.

AP6.6.1.3. Relationship verb phrases will be written in lowercase, normal font (Arial 10) type.

AP6.6.1.4. A legend will be displayed in the upper left corner of the model, with the following information:

Model Name
View Name
"As of" Date
DoD DAd Tracking # (assigned by the DoD DAd)

Presentation Legend:

BOLD = Approved
ITALICS = Candidate
NORMAL = Developmental
* = for display purposes only

AP6.6.1.5. Only entities and attributes found in the DoD data dictionary with approved, candidate, or developmental status will be displayed in the model; the model will contain as little

developmental status data as possible (only high level data, as necessary).

AP6.6.1.6. Entities shown “For Display Purposes Only” will contain all of their respective approved and candidate attributes.

AP6.6.1.7. Only entities that directly affect or are directly affected by proposed entities and attributes will be displayed for context. When a foreign key is displayed for context in a proposed entity, the entity from which the foreign key migrated will be displayed.

AP6.6.2. When the cross functional review package is prepared for distribution, the DoD DAd will ensure the ERD conforms to the guidelines. The submitter of the proposal package is required to prepare the ERD in conformance with the minimum guidelines as stipulated in C5. Chapter 5 and AP8. Appendix 8.

AP6.7. IMPLEMENTATION CONSIDERATIONS

The following conditions, if present in a logical data model, may pose implementation problems:

AP6.7.1. The attributes in the primary key contain a generic element of NAME or TEXT. Avoid primary keys containing textual domains.

AP6.7.2. More than four attributes appear as a concatenated primary key. When four or more attributes are required as a primary key, an alternate representation may be more appropriate.

AP6.7.3. The foreign key appears in more than three levels of dependent entities. This may indicate the model is hierarchical in nature and may not accurately reflect the business rules.

AP6.7.4. Indicator codes such as Y=YES; N=NO, or 1=Positive; 2=Negative are used. These values can often be derived from other data and should be used only in situations where database performance warrants their creation or where a business information requirement exits.

AP7. APPENDIX 7

ALTERNATIVE DATA STANDARDIZATION DEVELOPMENT ACTIVITIES

AP7.1. COLLABORATIVE SESSION

AP7.1.1. The collaborative session is held in support of the requirements definition activity. These sessions, which are an iterative process, promote joint modeling of the multiple, existing DoD information systems and expedite the data standardization approval process. These sessions result in a proposal package for an expedited cross functional review. The technical review and issue resolution occurs at the collaborative session(s). Therefore, there is no separate technical review of the proposed data standards. A representative of the DoD DAd is present at these sessions to provide information on existing entities and attributes in the model, and to ensure compliance of the new candidate entities and attributes with the appropriate standards.

AP7.1.2. The goal of these sessions is to minimize the amount of time required to prepare a proposal package for submission to the formal review process. Functional stakeholders and SMEs work together to prepare, review, and resolve issues related to proposed data standards. The process consists of two basic steps:

AP7.1.2.1. Identify and Select Projects

AP7.1.2.1.1. Candidate projects are nominated by FDAds and CDAds based on important migration system, functional and/or cross functional standard data, and/or Business Process Reengineering requirements.

AP7.1.2.1.2. Each project selected will have a migration system or application topic (e.g., Global Command and Control System (GCCS)) and a data topic (a DDM subject area, e.g., Location).

AP7.1.2.1.3. Each project selected will extend a subject area portion of the DDM in sufficient detail to ensure that data requirements of the system and/or application at issue are represented and can be standardized.

AP7.1.2.1.4. Candidate projects are reviewed and selected by the DoD DAd based on project scope, duration, functional and cross functional importance to DoD, quality and quantity of available documentation, expertise of participants, and return on investment for the DoD.

AP7.1.2.2. Plan and Hold Collaborative Sessions

AP7.1.2.2.1. Collaborative sessions are planned by FDAds, CDAds, and the DoD DAd. Meetings are held to identify what information exists, prioritize subfunctional and interfacing areas to be addressed, identify and prioritize preparatory tasks, set a schedule, and identify who, at a minimum, needs to be involved.

AP7.1.2.2.2. Data administration representatives with input from the co-chairs plan the sessions, facilities, and an agenda to accommodate and facilitate representative participation.

AP7.1.2.2.3. Projects are managed by the DoD DAd representative and facilitated by an impartial third party.

AP7.1.2.2.4. Projects are controlled by stringent timelines agreed to by the co-chairs and implemented by the DoD DAd representative and the facilitator.

AP7.1.2.2.5. Participants will provide pertinent documentation 10 days before the session and co-chairpersons will consolidate the information and provide copies to the participants before each session.

AP7.1.2.2.6. Participants will have the authority to represent their organizations in situations requiring technical and functional decisions.

AP7.1.2.2.6.1. The DoD DAd representative will be the decision authority for all procedural or technical issues.

AP7.1.2.2.6.2. The FDAd, who has stewardship over the subject area that is the data topic for the data standardization project, shall be the decision authority for intrafunctional or cross functional issues.

AP7.1.2.2.7. Issue resolution outside the data standardization collaborative session will be kept to a minimum. Issues that will be decided outside the collaborative sessions include:

AP7.1.2.2.7.1. Issues that adversely affect readiness or inability to comply with the law. These issues will be tabled and brought to the attention of the appropriate OSD PSA for resolution.

AP7.1.2.2.7.2. Data stewardship assignment and conflicting functional and technical issues. These issues will

be documented and brought to the attention of the DoD DAd for resolution within 48 hours.

AP7.1.2.2.7.3. Issues that cannot be resolved by participants in the collaborative session. When a resolution is unattainable, it will be brought to the attention of the ASD(C3I).

AP7.1.2.2.8. The output of a collaborative session is functionally and technically reviewed candidate data standards ready for cross functional review.

AP7.2. FOCUS SESSION

The focus session provides a mechanism to address a small subset of a proposal package during the cross functional review process. These sessions provide a focused and smaller audience session than a collaborative session. The DoD DAd identifies the Functional or Component areas to be represented to address the specific cross functional issue. The general steps in performing a focus session are:

AP7.2.1. Focus sessions are planned by the proposal package originator and supporting DoD DAd designated participants. Meetings are held to identify what information exists, set a schedule, and identify who, at a minimum, needs to be involved.

AP7.2.2. The DoD DAd representatives, with input from the proposal package originator, plan the sessions, schedule the facilities, and develop an agenda to accommodate and facilitate representative participation.

AP7.2.3. Issue resolution is controlled by stringent timelines agreed to by the leader and implemented by the DoD DAd representative and the facilitator.

AP7.2.4. Participants provide pertinent documentation 10 days prior to the session. The proposal package originator will consolidate the information and provide copies to the participants before the session.

AP7.2.5. Participants shall have the authority to represent their organizations in situations requiring technical and functional decisions.

AP7.2.6. The DoD DAd representative will be the decision authority for all procedural or technical issues.

AP7.2.7. The FDAd assigned stewardship for the candidate data standards shall be the decision authority for intrafunctional or cross functional issues.

AP7.2.8. The output of a focus session is the resolution of the cross functional issue.

AP8. APPENDIX 8

PROPOSAL PACKAGE PREPARATION

AP8.1. INTRODUCTION

This activity describes the preparation of a data standards proposal package. The FDAd will oversee the assembly of a package that proposes the functionally coordinated developmental data standards as an extension or update to the DDM. The proposal package should generally contain no more than 20 entities and 200 attributes. When a logical data model is being developed that is larger than 20 entities and 200 attributes, it should be partitioned into separate views that can be submitted as individual proposal packages. For details on the recommended tool set, refer to AP9. Appendix 9

AP8.2. DATA ELEMENT PROPOSAL PACKAGE

Each proposal package must contain the following:

AP8.2.1. Electronic Copy Of Logical Data Model (in IDEF1X). The model must:

AP8.2.1.1. Be normalized to third normal form (3NF).

AP8.2.1.2. Include meaningful verb phrases in named entity relationships (business rules).

AP8.2.1.3. Include labels for all discriminators or category indicators.

AP8.2.1.4. Include at least two subtype entities for each supertype entity for a complete categorization. (Refer to AP6. Appendix 6.)

AP8.2.1.5. Follow the naming convention for role names. (Refer to AP6. Appendix 6.)

AP8.2.1.6. Follow the naming convention for associative entities. (Refer to AP6. Appendix 6.)

AP8.2.1.7. Include any entity and its primary key from the DDM that has a relationship to a proposed entity in the logical data model, to indicate where the logical data model integrates into the DDM. These are annotated with an asterisk (“*”) at the beginning of the entity and primary key names to indicate “for

display purposes only". Entities and their primary keys contained in the model "for display purposes only" must be in approved or candidate status in the DoD data dictionary.

AP8.2.1.8. Include at least one native attribute for each entity. Each entity should have at least one attribute that originates from that entity (excluding associative entities).

AP8.2.2. Electronic Copy (ASCII) Listing Of Entities And Data Elements Contained in the Proposed Logical Data Model. This list must include:

AP8.2.2.1. DoD data dictionary counter identifiers.

AP8.2.2.2. DoD data dictionary version numbers.

AP8.2.2.3. Names.

AP8.2.2.4. Data Steward FDAds.

AP8.2.2.5. Functional area identifiers.

AP8.2.3. Proposed Changes to Existing Data Standards. When applicable, electronic copy (ASCII) listing of proposed changes to existing data standards (logical data models and meta-data). For each proposed modification to existing standards, this list must include:

AP8.2.3.1. DoD data dictionary counter identifier.

AP8.2.3.2. DoD data dictionary version number.

AP8.2.3.3. Name.

AP8.2.3.4. Data Steward FDAds.

AP8.2.3.5. Functional area identifiers.

AP8.2.3.6. A description of the changes to the current data standards (logical data models and meta-data).

AP8.2.3.7. A list of IS(s) where the existing data standard has been implemented. This information is available or should be recorded in the DoD data dictionary.

AP8.2.4. Archival of Existing Data Standards. For each request for archival of existing data standards, this list must include:

AP8.2.4.1. DoD data dictionary counter identifier.

AP8.2.4.2. DoD data dictionary version number.

AP8.2.4.3. Name.

AP8.2.4.4. Data Steward FDAds.

AP8.2.4.5. Functional area identifiers.

AP8.2.4.6. Rationale for archival.

AP8.2.4.7. A list of IS(s) where the existing data standard has been implemented. This information is available or should be recorded in the DoD data dictionary.

AP8.2.5. Cover Letter Signed By The FDAd. The letter will contain the following administrative information:

AP8.2.5.1. The sponsoring organization, is the organization that developed the proposal.

AP8.2.5.2. The model originator and/or point of contact, is the person who is representing the sponsoring organization.

AP8.2.5.2.1. Name.

AP8.2.5.2.2. Address.

AP8.2.5.2.3. Phone number.

AP8.2.5.2.4. Fax number.

AP8.2.5.2.5. E-mail address.

AP8.2.6. IS Being Supported. Information needed to prioritize proposal package processing by the DoD DAd. If applicable, provide the following:

AP8.2.6.1. IS name.

AP8.2.6.2. IS type (migration, developmental, other).

AP8.2.6.3. Completion and/or deployment date.

AP8.2.7. Modeling Tool Used to Create Proposed Model.

AP8.2.7.1. Tool name.

AP8.2.7.2. Tool version number.

AP8.2.8. DDM Information.

AP8.2.8.1. DDM Version used to create proposed model.

AP8.2.8.2. DDM view name.

AP8.2.9. Certification. Certification stating that:

AP8.2.9.1. Coordination has occurred with the appropriate organizations. Refer to C5. Chapter 5, Section C5.3., for detailed information on the coordination process.

AP8.2.9.2. All proposed data has been compared against existing approved and candidate data standards captured in the DoD data dictionary and only new requirements are contained in the proposal package.

AP8.2.9.3. All proposed data has been entered into the DoD data dictionary.

AP8.2.9.4. All data elements using the class word “IDENTIFIER” and proposed as primary key attributes represent “real world” identifiers and are unique across the DoD. The justification for the use of an identifier as a primary key and the method for creating and maintaining the identifier is contained in the Authority Reference Text or Comment Text.

AP8.2.9.5. All data elements with a specific domain have their complete set of domain values documented in the DoD data dictionary. All data elements using the class word “CODE” must have a specific domain.

AP8.2.10. Submitting FDAd Information. The FDAd submits the data standards proposal package to the DoD DAd for technical review and cross functional coordination with the following information:

AP8.2.10.1. Name.

AP8.2.10.2. Address.

AP8.2.10.3. Phone number.

AP8.2.10.4. Fax number.

AP8.2.10.5. E-mail address.

AP8.3. GENERIC ELEMENT PROPOSAL PACKAGE

Generic elements are centrally controlled and maintained by the DoD DAd in the DoD data dictionary. Proposals for new generic elements must be submitted to the DoD DAd for coordination and approval. They are submitted via a proposal package and their meta-data entered in the DoD data dictionary in accordance with the procedures in the document. However, since a generic element has no functional meaning by itself, no data model is necessary or required.

AP8.3.1. Proposal Package Contents. The proposal package must contain the following in electronic copy (ASCII):

AP8.3.1.1. DoD data dictionary counter identifier.

AP8.3.1.2. DoD data dictionary version number.

AP8.3.1.3. Generic element name.

AP8.3.1.4. Description of changes to existing generic element, or rationale for adding a new generic element.

AP8.3.1.5. Sponsoring Organization - is the organization that developed the proposal.

AP8.3.1.6. Certification from the originator that appropriate generic element meta-data has been entered into the DoD data dictionary.

AP9. APPENDIX 9

RECOMMENDED TOOL SET

AP9.1. INTRODUCTION

AP9.1.1. Objectives. The objectives of the recommended tool set are to:

AP9.1.1.1. Enable developers to build and maintain information systems that use and produce standard, interoperable data.

AP9.1.1.2. Minimize the cost of implementing DoD data standards.

AP9.1.1.3. Make the tools readily accessible to the data administration community. Detailed information on accessing the tools is available on the DoD Data Administration Home Page at: http://www-datadmn.itsi.disa.mil/tools.html.

AP9.1.2. Components. The current components of the tool set are the Defense Data Model (DDM); the Defense Data Dictionary System (DDDS); the PC Access Tool (PCAT); the Secure Intelligence Data Repository (SIDR); CD-ROM Data Standardization Support Tools; and Reference Data Sets on the World Wide Web (WWW). The tool set will evolve as needs change and technologies change to support tomorrow's needs.

AP9.2. DDM

The DDM represents the current data structures for the Department of Defense. The data is depicted graphically through the Entity Relationship Diagramming (ERD) technique using the ERwin data modeling tool. ERwin utilizes the IDEF1X syntax, which is the DoD adopted information modeling standard.

AP9.3. DDDS

The DDDS is the authoritative source of DoD data standards and is the mechanism to be used in the data standardization approval process. The purpose of the DDDS is to:

AP9.3.1. Provide developers approved standard elements.

AP9.3.2. Provide world-wide on-line query and reporting.

AP9.3.3. Collect and store standard elements and attributes.

AP9.3.4. Provide review and approval of standards functionally by the FDAd and technically by the DoD DAd.

AP9.3.5. Identify DoD organizations and processes using the standard elements.

AP9.3.6. Provide the capacity to track the state of standard element throughout their life cycle.

AP9.3.7. Provide File Transfer Protocol (FTP) access to the DDM.

AP9.4. PCAT

AP9.4.1. The PCAT is the stand-alone PC version of the DDDS. It provides a mechanism for defining meta-data, cross-referencing and consistency checking, and supports the standardization of data element names, definitions, and relationships.

AP9.4.2. PCAT is thesaurus-based and provides upload and download capability to the DDDS. It has been programmed using Visual Basic, and reposes within a Microsoft Access database.

AP9.4.3. PCAT is distributed on CD-ROM and recommended to be run on at least an Intel 486 PC platform.

AP9.5. SIDR

The SIDR is a classified version of the DDDS to support standardization of classified data elements and domains. The Functional proponent of this repository is the National Security Agency (NSA).

AP9.6. CD-ROM DATA STANDARDIZATION SUPPORT TOOLS

This CD contains the following data standardization support tools:

AP9.6.1. DDM. Described in AP9.2.

AP9.6.2. Command and Control (C2) Core Data Model. The C2 Core Data Model represents the core data required across all C2 functional activities and establishes a common approach to describing and implementing systems that support tactical C2 information requirements.

AP9.6.3. ERwin Viewer. The ERwin Viewer allows you to view IDEF1X data models in a view only format.

AP9.6.4. PCAT. Described in AP9.4.

AP9.6.5. Integration and Runtime Specification (I&RTS) for the Defense Information Infrastructure (DII) Common Operating Environment (COE). The I&RTS describes the technical requirements for using the DII COE to build and integrate systems. It provides implementation details that describe, from a software development perspective, the following:

AP9.6.5.1. The COE approach to software reuse;

AP9.6.5.2. The COE runtime execution environment;

AP9.6.5.3. The definition and requirements for achieving COE compliance;

AP9.6.5.4. The process for automated software integration; and

AP9.6.5.5. The process for electronically submitting and retrieving software components to or from the COE software repository.

AP9.7. REFERENCE DATA SETS

AP9.7.1. Description. Reference data sets provide the uniform representation of reference data that are approved for use in DoD systems. They are based on DoD data standards approved for use in accordance with the procedures delineated in this manual. Reference data sets are designed to facilitate the use and reuse of relatively static data found in code tables. Examples include: Country Code; US State Code; Purchase Order Type Code; and Security Classification Code.

AP9.7.2. Contents. Reference data sets consist of the following reusable software components: logical and physical data models; SQL Create Table Statements; ASCII files of domain values (codes and definitions), and load scripts.

AP9.7.3. Access. Detailed information on accessing approved reference data sets is available on the DII/COE Home Page at: http://diides.ncr.disa.mil/shade/.